Vol. No. 1 CONNECTICUT INSURANCE LAW

Pages 1–316

CONNECTICUT INSURANCE LAW JOURNAL

ARTICLES

Volume 28 2021–2022 Number 1

CONNECTICUT INSURANCE LAW JOURNAL

Volume 28, Number 1
Fall 2021

University of Connecticut School of Law
Hartford, Connecticut

Connecticut Insurance Law Journal (ISSN 1081-9436) is published at least twice a year by the Connecticut Insurance Law Journal Association at the University of Connecticut School of Law. Periodicals postage paid at Hartford, Connecticut. Known office of publication: 55 Elizabeth Street, Hartford, Connecticut 06105-2209. ***Printed by: Joe Christensen, Inc., 1540 Adams Street, Lincoln, Nebraska 68521.***

Please visit our website at http://www.insurancejournal.org or see the final page of this issue for subscription and back issue ordering information.

Postmaster: Send address changes to Connecticut Insurance Law Journal, 55 Elizabeth Street, Hartford, Connecticut 06105-2209.

The Journal welcomes the submission of articles and book reviews. Both text and notes should be double or triple-spaced. Submissions in electronic form are encouraged and should be in Microsoft™ Word™ version 97 *format or higher. Citations should conform to the most recent edition of* A UNIFORM SYSTEM OF CITATION, *published by the Harvard Law Review Association.*

It is the policy of the University of Connecticut to prohibit discrimination in education, employment, and in the provision of services on the basis of race, religion, sex, age, marital status, national origin, ancestry, sexual preference, status as a disabled veteran or veteran of the Vietnam Era, physical or mental disability, or record of such impairments, or mental retardation. University policy also prohibits discrimination in employment on the basis of a criminal record that is not related to the position being sought; and supports all state and federal civil rights statutes whether or not specifically cited within this statement.

Cite as CONN. INS. L.J.

CONNECTICUT INSURANCE LAW JOURNAL

VOLUME 28 2021–2022 NUMBER 1

UNIVERSITY OF CONNECTICUT
SCHOOL OF LAW

FACULTY AND OFFICERS OF ADMINISTRATION
FOR THE ACADEMIC YEAR 2021–2022

Officers of Administration

Radenka Maric, Ph.D., *Interim President, University of Connecticut*
Carl W. Lejuez, Ph.D., *Provost and Executive Vice President for Academic Affairs*
Eboni S. Nelson, J.D*., Dean, School of Law*
Paul Chill, J.D., *Associate Dean for Academic Affairs and Clinical Professor of Law*
Jennifer Mailly, J.D., *Associate Dean for Experiential Education, Clinical Professor of Law and Field Placement Program Director*
Richard A. Wilson, BSc., Ph.D., *Associate Dean for Faculty Development and Intellectual Life*
Jennifer Cerny, J.D., *Executive Director of Student Affairs & Assistant Dean of Students*
Karen L. DeMeola, J.D., *Assistant Dean for Finance, Administration and Enrollment*

Faculty Emeriti

Robin Barnes, B.A., J.D., *Professor of Law Emerita*
Loftus E. Becker, Jr., A.B., LL.B., *Professor of Law Emeritus and Oliver Ellsworth Research Professor of Law*
John C. Brittain, B.A., J.D., *Professor of Law Emeritus*
Deborah A. Calloway, B.A., J.D., *Professor of Law Emerita*
Clifford Davis, S.B., LL.B., *Professor of Law Emeritus*
Timothy H. Everett, B.A., M.A., *Clinical Professor of Law Emeritus*
Richard S. Kay, A.B., M.A., J.D., *Wallace Stevens Professor of Law Emeritus and Oliver Ellsworth Research Professor of Law*
Lewis S. Kurlantzick, B.A., LL.B., *Zephaniah Swift Professor of Law Emeritus and Oliver Ellsworth Research Professor of Law*
Patricia A. McCoy, B.A., J.D., *Professor of Law Emerita*
R. Kent Newmyer, Ph.D., *Professor of Law and History Emeritus*
Nell J. Newton, B.A., J.D., *Dean and Professor of Law Emerita*
Jeremy R. Paul, A.B., J.D., *Dean and Professor of Law Emeritus*
Eileen Silverstein, A.D., J.D., *Professor of Law Emerita*
James H. Stark, A.B., J.D., *Roger Sherman Professor of Law Emeritus and Oliver Ellsworth Research Professor*
Kurt A. Strasser, B.A., J.D., LL.M., J.S.D., *Phillip Blumberg Professor of Law Emeritus*
Colin C. Tait, B.A., LL.B., *Professor of Law Emeritus*
Carol Ann Weisbrod, J.D., *Professor of Law Emerita*
Nicholas Wolfson, A.B., J.D., *Professor of Law Emeritus*

Faculty of Law

Jill C. Anderson, B.A., University of Washington; J.D., Columbia University; *Professor of Law*
Jon Bauer, B.A., Cornell University; J.D., Yale University; *Clinical Professor of Law and Richard D. Tulisano '69 Human Rights Scholar*
Mary Beattie, B.A., Providence College; J.D., University of Bridgeport; *Assistant Clinical Professor of Law and Director, Academic Support*
Bethany Berger, B.A., Wesleyan University; J.D., Yale University; *Wallace Stevens Professor of Law*
Robert L. Birmingham, A.B., J.D., Ph.D. (Econ.), Ph.D. (Phil.), University of Pittsburgh; LL.M., Harvard University; *Professor of Law*
Kiel Brennan-Marquez, B.A., Pomona College; J.D., Yale University; *Associate Professor of Law and William T. Golden Scholar and Faculty Director of the Center on Community Safety, Policing and Inequality*
Paul Chill, B.A., Wesleyan University; J.D., University of Connecticut; *Associate Dean for Academic Affairs and Clinical Professor of Law*

John A. Cogan, Jr., B.A., University of Massachusetts Amherst; M.A., University of Texas; J.D., University of Texas School of Law; *Associate Professor of Law and Roger S. Baldwin Scholar*

Mathilde Cohen, B.A., M.A., L.L.B., Sorbonne-École Normale Supérieure; LL.M., J.S.D., Columbia University; *George Williamson Crawford Professor of Law*

Tara Cooley, B.S., Meredith College; M.P.A. University of Nevada Las Vegas; J.D., Golden Gate University; L.L.M., Lewis & Clark Law School; *Teaching Fellow*

Diane F. Covello, B.S., University of Kansas; J.D., Duke University School of Law; *Co-Director, Intellectual Property and Entrepreneurship Law Clinic and Assistant Clinical Professor of Law*

Anne C. Dailey, B.A., Yale University; J.D., Harvard University; *Evangeline Starr Professor of Law*

Miguel F. P. de Figueiredo, B.A., Johns Hopkins University; M.A., University of Chicago; Ph.D., University of California, Berkeley; J.D., Yale University; *Associate Professor of Law and Terry J. Tondro Research Scholar*

Jessica de Perio Wittman, B.A., State University of New York at Stony Brook; B.A, M.L.S., State University of New York at Buffalo; J.D., Seattle University School of Law; *Director of the Law Library*, *Associate Professor of Law and Cornelius J. Scanlon Scholar*

Todd D. Fernow, B.A., Cornell University; J.D., University of Connecticut; *Professor of Law and Director, Criminal Law Clinic*

Richard Michael Fischl, B.A., University of Illinois; J.D., Harvard University; *Professor of Law*

Timothy Fisher, B.A., Yale University; J.D., Columbia University; *Dean Emeritus and Professor of Law*

Valeria Gomez, B.A., Belmont University; J.D., University of Tennessee College of Law; *Visiting Assistant Clinical Professor of Law and William R. Davis Clinical Teaching Fellow*

Hillary Greene, B.A., J.D., Yale University; *Zephaniah Swift Professor of Law*

An-Ping Hsieh, B.A, Yale University, J.D., Boston College Law School; *Visiting Professor from Practice*

Nadiyah J. Humber, B.S., Vanderbilt University; J.D., Suffolk University School of Law; *Associate Professor of Law*

Mark W. Janis, A.B., Princeton University; B.A., M.A., Oxford University; J.D., Harvard University; *William F. Starr Professor of Law*

Maureen Johnson, M.F.A., UCLA; J.D., Loyola Law School*; Assistant Clinical Professor of Law*

Darcy Kirk, A.B., Vassar College; M.S., M.B.A., Simmons College; J.D., Boston College; *Distinguished Professor of Law*

Peter R. Kochenburger, A.B., Yale University; J.D., Harvard University; *Associate Clinical Professor of Law, Executive Director of the Insurance LL.M. Program and Deputy Director of the Insurance Law Center*

James Kwak, A.B., Harvard College; Ph.D., University of California at Berkeley; J.D., Yale Law School; *Jesse Root Professor of Law*

Alexandra D. Lahav, A.B., Brown University; J.D., Harvard University; *Ellen Ash Peters Professor of Law*

Molly K. Land, B.A., Hamline University; J.D., Yale; *Catherine Roraback Professor of Law*

Leslie C. Levin, B.S.J., Northwestern University; J.D., Columbia University; *Hugh Macgill Professor of Law*

Peter L. Lindseth, B.A., J.D., Cornell University; M.A., M. Phil, Ph.D., Columbia University; *Olimpiad S. Ioffe Professor of International and Comparative Law and Director, Graduate, International, and Non-JD Programs*

Richard Luedeman, A.B.; Harvard University; J.D.; Yale Law School; *Assistant Clinical Professor of Law*

Joseph A. MacDougald, A.B., Brown University; M.B.A., New York University; J.D., University of Connecticut; M.E.M., Yale University; *Professor-in-Residence; Executive Director, Center for Energy and Environmental Law*

Jennifer Brown Mailly, A.B., Brown University; J.D., Ohio State University; *Associate Dean for Experiential Education, Clinical Professor of Law and Field Placement Program Director*

Willajeanne F. McLean, B.A., Wellesley College; B.S., University of Massachusetts; J.D., Fordham University; LL.M., Free University of Brussels; *Distinguished Professor of Law*

Thomas H. Morawetz, A.B., Harvard College; J.D., M.Phil., Ph.D., Yale University; *Tapping Reeve Professor of Law and Ethics*

Minor Myers, B.A., Connecticut College; J.D., Yale University; *Professor of Law*
Eboni S. Nelson, B.A., Wake Forest University; J.D., Harvard Law School; *Dean and Professor of Law*
Ángel R. Oquendo, A.B., M.A., Ph.D., Harvard University; J.D., Yale University; *George J. and Helen M. England Professor of Law*
Sachin S. Pandya, B.A., University of California, Berkeley; M.A., Columbia University; J.D., Yale University; *Professor of Law*
Travis Pantin, B.A., University of Chicago; J.D., Yale Law School; *Director of the Insurance Law Center and Associate Professor of Law*
Lisa Perkins, B.S., J.D., Michigan State University; LL.M., Georgetown University Law Center; *Clinical Professor of Law and Director, Tax Clinic*
Richard D. Pomp, B.S., University of Michigan; J.D., Harvard University; *Alva P. Loiselle Professor of Law*
Jessica S. Rubin, B.S., J.D., Cornell University; *Clinical Professor of Law and Director, Legal Practice Program*
Susan R. Schmeiser, A.B., Princeton University; J.D., Yale University; Ph.D., Brown University; *Professor of Law*
Peter Siegelman, B.A., Swarthmore College; M.S.L., Ph.D., Yale University; *Phillip I. Blumberg Professor of Law*
Julia Simon-Kerr, B.A., Wesleyan University; J.D., Yale Law School; *Professor of Law*
Rachel Timm, B.A., University of Nebraska; J.D., Creighton School of Law; *Assistant Clinical Professor of Law*
Stephen G. Utz, B.A., Louisiana State University; J.D., University of Texas; Ph.D., Cambridge University; *Roger Sherman Professor of Law*
Anna VanCleave, M.A., University of Michigan; J.D., NYU School of Law; *Director of the Criminal Defense Clinic and Associate Professor of Law*
Steven Wilf, B.S., Arizona State University; Ph.D., J.D., Yale University; *Anthony J. Smits Professor of Global Commerce*
Richard A. Wilson, BSc., Ph.D., London School of Economics and Political Science; *Associate Dean for Faculty Development and Intellectual Life, Gladstein Chair of Human Rights and Board of Trustees Distinguished Professor of Law and Anthropology*
Carleen Zubrzycki, B.A., Yale University; J.D., Yale School of Law; *Associate Professor of Law*

CONNECTICUT INSURANCE LAW JOURNAL

VOLUME 28 2021–2022 NUMBER 1

CONTENTS

ARTICLES

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

H. BRYAN CUNNINGHAM[*]
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

---

[*] 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.

exclusions in cyber insurance coverage disputes. We offer a prioritized and 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 (defining 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 disasters. This reality is artificially distorting the cyber insurance ecosystem.

---

[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. 967, 1015–17 (2021).

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. 1 (2021); Josephine Wolff, *"Cyberwar By Almost Any Definition": NotPetya, the Evolution of Insurance War Exclusions, and Their Application to Cyberattacks*, 28 CONN. INS. L. J. 85 (2021); Scott J. Shackelford, *Wargames: Analyzing the Act of War Exclusion in Cyber Risk Insurance Coverage and Its Implications for Cybersecurity Policy*, 23 YALE L. J. & TECH. 362 (2021); Shauhin A. Talesh, *How*

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

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.

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 silent cyber insurance risk"[14] (our proposal would only provide government financial backstopping for "stand-alone" cyber policies or policies otherwise

---

[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, N.Y. 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.

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

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.

---

[15] *Id.*

[16] *Id.*

[17] Letter from Linda A. Lacewell, *supra* note 13. *See 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 this 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 35 (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 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 4 (footnote omitted). Abraham and Schwarcz note, however, that, "[o]f course, not all of a future cyber catastrophe's costs will be insured. But a central message of this Article is that a much larger portion of these costs could prove to be covered than is currently 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 4 (footnotes 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 1015–17.

[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 1005.

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 976, 1005–07.

[45] *Id.* at 1007–11.

[46] *Id.* at 1011–14

[47] In fact, our research reveals very few buyers of cyber insurance use insurer-sponsored pre-breach services. *Id.* at 1115.

> 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 8.

[51] These numbers are slightly higher than in some recent surveys. *See, e.g.*, *id.* at 45 ("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.'" (footnote 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) (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 publication focused on the potential effects of attempted enforcement of war exclusions, one scholar notes that: "[a]mong the most vexing issues, with arguably wide-ranging implications for not only the cyber risk insurance industry, but for U.S. cybersecurity policy generally, consist of when a cyber attack attributed 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 362.

[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 28 (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, at 382–85; *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

---

[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.

determinations predictable, further undermining rational cyber insurance ecosystem stabilization.

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

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

> 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 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 and Schwarz observed, in support of a government insurance backstopping program, that "[t]he social benefits of such coverage likely extend further, as insurance 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

---

[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.

improve the cybersecurity of the U.S. private sector and the security of the nation as a whole in cyberspace.[107]

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

---

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

[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 CSC REPORT, *supra* note 2, for a further discussion of recent global hacker activities.

hearings, that even leaders of companies most likely to be regulated are now supportive of such regulation.[111]

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

---

[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, 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. (Apr. 28, 2021), https://www.gmfus.org/publications/quantifying-risk-innovative-approaches-cybersecurity; Shackelford, *supra* note 8, at 412–13; Abraham & Schwarcz, *supra* note 8.

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 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 I.

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[129] and other commentators 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 62–66.
[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. *See 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

---

[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.

includes cyber insurance coverage as part of, or an endorsement to, the policy—

(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 41 ("[T]he vast majority of global cloud services outside of 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-

> 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]

---

attack-february/ (discussing the 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

---

[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), https://www.forbes.com/sites/marshallshepherd/2019/10/10/a-trillion-dollar-storm-looms-for-earth-and-its-not-a-hurricane/?sh=eb216136ebcc (citing Robert Coker, *The Trillion-Dollar (Solar) Storm*, SPACE REV. (Oct. 30, 2017), https://www.thespacereview.com/article/3358/1).

> now with regard to NotPetya. Zurich doesn't want to pay a 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).

"CYBERWAR BY ALMOST ANY DEFINITION"[1]: NOTPETYA, THE EVOLUTION OF INSURANCE WAR EXCLUSIONS, AND THEIR APPLICATION TO CYBERATTACKS

JOSEPHINE WOLFF[*]

TABLE OF CONTENTS

INTRODUCTION

In June 2017, the multinational food company Mondelez International Inc. ("Mondelez") was hit by the NotPetya ransomware virus.[2] NotPetya exploited a vulnerability in the Microsoft Windows operating system to encrypt the contents of infected computers' hard drives[3] and demanded a ransom payment of roughly $300 worth of bitcoins before it would turn the contents of the computers back over to their owners.[4]

---

[1] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

[*] Associate Professor of Cybersecurity Policy, Tufts University Fletcher School of Law and Diplomacy. I am grateful to Daniel Schwarcz, Daniel Woods, and participants in the symposium on The Role of Law and Government in Cyber Insurance Markets co-hosted by the University of Connecticut School of Law and University of Minnesota Law School for their helpful comments and suggestions.

[2] Complaint & Demand for Jury Trial at 2, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008 (Ill. Cir. Ct. Oct. 10, 2018) [hereinafter Mondelez Complaint].

[3] CITI GPS, MANAGING CYBER RISK WITH HUMAN INTELLIGENCE: A PRACTICAL APPROACH 24, 28 (Global Perspective & Solutions May 2019 ed., 2019).

[4] Matt Burgess, *What Is the Petya Ransomware Spreading Across Europe? WIRED Explains*, WIRED (Mar. 7, 2017, 10:35 AM), https://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017.

NotPetya infiltrated more than 2,000 organizations worldwide during the summer of 2017,[5] including Mondelez, which had to shut down 1,700 servers and 24,000 laptops due to NotPetya infections.[6] In the aftermath of the incident, Mondelez filed a claim with its insurer, Zurich American Insurance Co. ("Zurich"), under its global property insurance policy, which covered "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 . . . ."[7] Zurich initially agreed to pay out $10 million to Mondelez to cover its losses but then changed its mind and refused to cover any of the costs on the grounds that NotPetya was a "hostile or warlike action" perpetrated by a "government or sovereign power" and thereby excluded from coverage.[8]

Mondelez filed a $100 million lawsuit against Zurich in October 2018[9] and the case (unresolved at the time of writing) raises difficult questions about what constitutes war (or "warlike" actions) in the online domain. Since the lines between online espionage, sabotage, and warlike attacks are often blurrier online than in the physical domain, classifying an incident like NotPetya as "warlike" is far from straightforward. While war is typically not a regular occurrence or routine concern for insurance holders, cyberattacks perpetrated by nation states are not uncommon,[10] and excluding them from coverage could place a significant burden on policyholders.[11] Moreover, the lengthy and sometimes contentious process of determining

---

[5] CITI GPS, *supra* note 3, at 23.

[6] Mondelez Complaint, *supra* note 2, at 2–3.

[7] *Id.* at 2.

[8] *Id.* at 4–6.

[9] *Id.* at 1, 10.

[10] MICHAEL GROSKOP, NISSIM PARIENTE, LOUIS SCIALABBA, EYAL ARAZI, & DANIEL SMITH, RADWARE, PROTECTING WHAT YOU CAN'T SEE: ELIMINATING SECURITY BLIND SPOTS IN AN AGE OF TECHNOLOGICAL CHANGE 5 (Deborah Szajngarten & Ben Zilberman eds., Global Application & Network Security Report 2019-2020 ed., 2020) ("Nation-state attacks were an issue as respondents indicated a substantial increase in the percentage of cyberattacks attributed to cyberwar, up from 19% in 2018 to 27% in 2019."). *See also* CITI GPS, *supra* note 3, at 16 ("Nation state actors conduct espionage to steal intellectual property and collect intelligence considered vital to advancing national interests. Challenging to detect and mitigate, these actors have substantial resources allocated to developing and sustaining sophisticated capabilities.").

[11] *See generally* Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe*, 27 CONN. INS. L.J. 1, 48 (2021) (discussing the lack of clarity of nation-state exclusions for policyholders).

who is behind a cyberattack and whether it can be definitively attributed to a nation state, adds to the challenges of interpreting this exception and applying it to online threats.[12] Additionally, since a single piece of malware like NotPetya may not only be used for a warlike purpose (e.g., shutting down the Ukrainian electric grid)[13] but can also cause significant collateral damage to unintended victims, such as Mondelez and other private entities,[14] it is not clear whether a war exclusion should apply to every incident caused by the same piece of malware or only to specific warlike components or impacts of that malware's effects.

Because NotPetya was the first public case of a cyberattack being deemed an act of war by insurers as grounds for denying a claim,[15] both insurers and policyholders have few directly analogous precedents to rely on in order to understand what these war exclusions do and do not apply to in the cyber domain.[16] However, while it may be the first cyberattack to land in court over its disputed warlikeness, NotPetya is not the first time that ambiguous incidents categorized by insurers as "war" or "warlike" have been challenged in court by policyholders.[17] In fact, the language of war exclusions in insurance policies, like that purchased by Mondelez, has been shaped by a series of historical inflection points when claims activity and subsequent lawsuits forced insurers to realize they needed to broaden or otherwise clarify what types of activities these exceptions applied to.[18] As buyers and sellers of cyber-insurance seek to better understand how these exclusions may apply to online attacks and intrusions, it may be helpful to

---

[12] *Id.* at 44–50.

[13] Thomas Brewster, *NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid'*, FORBES (July 3, 2017, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/.

[14] Adam Satariano & Nicole Perloth, *Big Companies Thought Insurance Covered a Cyber Attack. They May Be Wrong*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

[15] Dominic T. Clarke, *Cyber Warfare and the Act of War Exclusion, in* GLOBAL LEGAL GROUP LTD., INTERNATIONAL COMPARATIVE LEGAL GUIDE: INSURANCE & REINSURANCE 2020 11, 12 (9th ed. 2020).

[16] Abraham & Schwarcz, *supra* note 11, at 48.

[17] *See, e.g.*, Pan Am. World Airways v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974); Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp. 1460 (S.D.N.Y. 1983); Sherwin-Williams Co. v. Ins. Co. of Pa., 863 F. Supp. 542 (N.D. Ohio 1994).

[18] *See generally* Josephine Wolff, Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks (Jan. 8, 2022) (unpublished manuscript) (on file with author).

consider the development and legal history of insurance war exclusions and what lessons that history offers about how such exclusions may be applied to cyberattacks in their current form or further refined to more directly address emerging online threats.

This article describes some of the stages of the evolution of war exclusions in insurance policies since the mid-twentieth century. It also considers what we can learn from the history of legal challenges to claims denied under these exclusions and about how courts and insurers are likely to interpret their relevance and application to cyberattacks like NotPetya. Specifically, this article looks at lawsuits resulting from the aftermath of Pearl Harbor, the 1970 hijacking of Pan American Flight 093, the destruction in 1975 of the Holiday Inn hotel in Beirut during a civil war, and explores how each incident changed the language used by insurers in drafting war exclusions to encompass increasingly broader categories of activity that could, conceivably, be interpreted as applying to many forms of cyberattacks and online intrusions, including NotPetya. Finally, this article argues that given the challenges of attribution, risk correlation, and determining the precise purpose of malware, war exclusions that apply to cyberattacks should not be predicated on being able to identify the perpetrator or motive of such attacks, but rather on their victims, impacts, and scale. However, this framing of war exclusions is, in many ways, directly contradictory to their evolution over the past century and may therefore be difficult to reconcile with existing language governing these exclusions.

I. ORIGINS OF WAR EXCLUSIONS & PEARL HARBOR

The exclusion Zurich pointed to in Mondelez's property insurance policy excluded losses or damage directly or indirectly caused by "hostile or warlike action in time of peace or war . . . ."[19] The practice of excluding war risks from all-risk insurance policies dates back more than one hundred years before NotPetya. Originally, in the nineteenth century maritime insurance policies had included coverage for losses at sea caused by wars—an issue of particular concern to ship owners since wars often affected marine voyages.[20] However, in 1898, Lloyd's Insurance Exchange ("Lloyds") added a Free of Capture & Seizure Clause ("FC&S") to its general marine cargo clause that excluded coverage for any losses caused by war. [21] As FC&S

---

[19] Mondelez Complaint, *supra* note 2, at 4.

[20] Helen M. Benzie, *War and Terrorism Risk Insurance*, 18 J.C.R. & ECON. DEV. 427, 428 (2004).

[21] *Id.* at 428–29.

clauses became standard practice, some insurers, including Lloyd's, also started offering coverage specifically for war risks, but the scale and unpredictability of losses caused by wars made it difficult for insurers to reliably model such policies or be certain they could cover the resulting claims.[22] In particular, the potential for wars to result in highly correlated risks posed significant challenges to insurers and continues to make these risks difficult for insurers to model and cover today. Accordingly, in 1913, a committee established by the British government determined that private insurers could not meet the demand for war insurance, and the government subsequently agreed to reinsure eighty percent of the war risks insurers underwrote.[23] Similarly, in the United States, Congress passed the War Risk Insurance Act in 1914, establishing the Bureau of War Risk Insurance in the Treasury Department to provide war risk coverage for marine commerce.[24] Thus, by the early twentieth century, war risks were already being excluded from standard forms of all-risk insurance and were understood to be uninsurable by the private market without support from policymakers.

War exclusions have evolved from their roots in marine insurance to become a common feature in other types of coverage, including property insurance and life insurance. Following the attack on Pearl Harbor in 1941, a series of lawsuits—mostly brought by the beneficiaries of life insurance policies for people killed during the attack—tested the meaning and limitations of this type of exclusion.[25] In particular, the fact that the attack on the morning of December 7, 1941, occurred one day prior to the United States' declaration of war against Japan, complicated the question of whether Pearl Harbor could be considered an act of war for insurance purposes.[26] For instance, when Navy seaman Howard A. Rosenau died at Pearl Harbor, his parents, Arthur and Freda Rosenau, filed a claim with Idaho Mutual Benefit Association ("Idaho Mutual"), where their son had purchased a $1,000 life insurance policy prior to his death and named them as beneficiaries.[27] Idaho Mutual denied the claim because Rosenau's policy included an exclusion for

---

[22] *See generally id.*

[23] *Id.* at 429.

[24] War Risk Insurance Act of 1914, Pub. L. No. 63-193, 38 Stat. 711 (1914) (repealed 1933).

[25] *See, e.g.,* Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687 (Mass. 1942); Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227 (Idaho 1944); Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208 (1945); N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260 (10th Cir. 1946).

[26] *Rosenau*, 145 P.2d at 228.

[27] *Id.* at 227–28.

"death, disability or other loss sustained while in military, naval, or air service of any country at war."[28]

Because the United States was not yet at war with Japan at the time of the Pearl Harbor attack, an Idaho court ruled in favor of Rosenau's parents, ordering Idaho Mutual to pay them the full amount due under their son's policy.[29] The insurer appealed this decision to the Idaho Supreme Court, arguing that the United States was already at war when Rosenau died at Pearl Harbor, and his death was therefore excluded from coverage.[30] To support this argument, Idaho Mutual cited the preamble of the resolution Congress adopted the day after Pearl Harbor, on December 8, 1941, titled *Joint Resolution declaring that a state of war exists between the Imperial Government of Japan and the Government and People of the United States*.[31] The preamble stated, "[w]hereas, the Imperial Government of Japan has committed unprovoked acts of war . . . . That the state of war between the United States and the Imperial Government of Japan, which has thus been thrust upon the United States is hereby formally declared . . . ."[32] Idaho Mutual argued that these references to the Pearl Harbor attack as an "unprovoked act of war" and a pre-existing "state of war" between the United States and Japan that was merely codified, not initiated, by Congress on December 8th, meant that the Pearl Harbor attack occurred in a "country at war."[33]

Arthur and Freda Rosenau disputed this broad interpretation of "war" that allowed for a country to be considered "at war" even prior to a formal declaration by its government.[34] They argued that if the court accepted the insurer's interpretation of what it meant to be "at war" then:

> [I]t would mean that the United States has been constantly at 'war' with Japan since the sinking of the gunboat Panay in China in the early 1930's, and it would mean that Russia and Japan are now at 'war' by virtue of the fact that within recent years there have been border patrol clashes and

---

[28] *Id.*
[29] *Id.* at 228.
[30] *Id.* at 228–29.
[31] *Id.* at 229. *See* S.J. Res. 116, 77th Cong. (1941).
[32] S.J. Res. 116.
[33] *Rosenau*, 145 P.2d at 229.
[34] *Id.* at 232.

> hostilities in some force along the border between Manchuria and Russian Siberia.[35]

Their point—a particularly poignant one for considerations of online warlike acts—was that a broad interpretation of what it meant to be "at war" could quickly expand to apply to many hostile attacks, not all of which would necessarily lead to actual wars that were officially declared as such by the nations involved.[36] They further argued,

> The Panay incident was a hostile attack, but it was atoned for. The border clashes between Russian and Japanese territory were unquestionably armed invasions of the other's territory. Yet they were atoned for and 'war' did not ensue. It was possible, no matter how improbable, that the Pearl Harbor attack could have been atoned for and adjusted without 'war' necessarily ensuing.[37]

The majority ruling of the Idaho Supreme Court was sympathetic to this line of reasoning, citing an international law textbook by John Bassett Moore that emphasized war as a "legal condition" such that "if two nations declare war one against the other, war exists, though no force whatever may as yet have been employed. On the other hand, force may be employed by one nation against another, as in the case of reprisals, and yet no state of war may arise."[38] The court majority was unwilling to deviate from this strict, legal definition of war in interpreting Rosenau's life insurance policy, writing in its 1944 ruling:

> It is true, as pointed out by appellant, that the word war, in a broad sense, is used to connote a state or condition of war, warlike activities, fighting with arms between troops, etc., but we are here concerned with the meaning and intent of the word as contained in a formal, legal contract of insurance, a class of contracts which the courts are very frequently called upon to consider and construe, and it

---

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.* at 229–30 (quoting 7 JOHN BASSET MOORE, A DIGEST OF INTERNATIONAL LAW 153 (1906)).

> seems quite obvious that words and phrases in a contract of this nature, are used and intended to be used in the legal sense.[39]

The Idaho Supreme Court determined that a ruling in favor of Idaho Mutual would mean interpreting the language in the life insurance policy not "in its accepted legal sense" but rather, as applying to "cases where conditions of war, or conditions which might lead to war, existed."[40] If it did that, the majority opinion pointed out, "the court would . . . be making a new contract for the parties, by adding to the contract phrases, terms and conditions, which it does not contain. This, of course, is not one of the functions of a court."[41]

Two justices on the Idaho Supreme Court dissented, arguing that the Pearl Harbor attack had, for all intents and purposes, been an act of war.[42] Justice James F. Ailshie wrote, "[w]here the armed forces of two sovereign nations strike blows at each other, as occurred at Pearl Harbor on December 7, 1941, and do so under the direction and authority of their respective governments, it is difficult for me to understand why that is not *war*."[43] Ailshie's rationale was based on the idea that Pearl Harbor looked like an act of war—not just to him, but also to "the average citizen, who might apply for and procure a life insurance policy [sic] . . . ."[44] To him, what determined whether a country was at war was not the legal status of that war but rather, whether a person witnessing a violent or hostile act would recognize it as such. Broadening the definition of war in this way was essential, Ailshie argued, because "[o]ur political history demonstrates that most wars have been commenced and prosecuted without any formal declaration of war; and that war dates from its inception rather than from the time on which some formal declaration to that effect is made."[45]

While the Rosenaus were ultimately successful in forcing their son's insurer to pay out his policy, other beneficiaries met with more mixed results. In 1942, two years before the final ruling in *Rosenau*, the Supreme Court of Massachusetts ruled against Marcella Stankus, who sought a life insurance payout from New York Life Insurance Co. ("New York Life Insurance")

---

[39] *Id.* at 230.

[40] *Id.*

[41] *Id.*

[42] *Id.* at 232–36 (Ailshie, J., dissenting) (with Justice Budge concurring with Justice Ailshie's dissent).

[43] *Id.* at 236.

[44] *Id.*

[45] *Id.*

following the death of her son, Anthony Stankus in 1941.[46] Anthony, like Howard Rosenau, was a Navy seaman, but he did not die at Pearl Harbor—instead, he died two months earlier on October 30, 1941, when his ship, the U.S.S. Reuben James, was sunk by a torpedo in the Atlantic Ocean.[47] The war exclusion in Stankus's life insurance policy, worded slightly more broadly than the one in Rosenau's policy, ruled out coverage for death resulting "directly or indirectly from . . . war or any act incident thereto."[48] Marcella Stankus, like Rosenau's parents, argued that since the United States had not declared war on October 30, 1941, at the time of Anthony's death, it could not be considered a death resulting from war.[49]

An early judgment by a lower court had agreed with that argument, holding that the insurer must pay out the full claim to Marcella Stankus, but when New York Life Insurance appealed that decision, the Supreme Judicial Court of Massachusetts sided with them, reversing the initial decision.[50] Justice James J. Ronan authored the 1942 opinion, writing, "the existence of a war is not dependent upon a formal declaration of war. Wars are being waged today that began without any declaration of war. The attack by the Japanese on Pearl Harbor on December 7, 1941, is the latest illustration."[51] Two years later, in his dissent in *Rosenau*, Ailshie seized on that line as evidence that the attack on Pearl Harbor should also count as an act of war because the Massachusetts court had already deemed it so when deciding *Stankus*.[52] Ultimately, the Massachusetts Court reached exactly the opposite conclusion of the Idaho Court, deciding, "the clause exempting the defendant from liability where death is caused by war is not restricted in its operation to a death that has resulted from a war being prosecuted by the United States."[53] Ailshie, in his *Rosenau* dissent, alluded to the fact that war was ongoing in Europe well before the United States' official declaration, raising the question of whether an officially declared conflict between some countries would suffice to satisfy the war exclusion, even if the resulting damage occurred in a different country.[54] This line of reasoning could be relevant for NotPetya as well since the malware was designed for the

---

[46] Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687 (Mass. 1942).
[47] *Id.* at 688.
[48] *Id.* at 687–88.
[49] *Id.* at 688.
[50] *Id.* at 688, 689–90.
[51] *Id.* at 688.
[52] Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227, 236 (Idaho 1944).
[53] *Stankus*, 44 N.E.2d at 689.
[54] *Rosenau*, 145 P.2d at 235–36.

ongoing conflict between Russia and Ukraine, but the damage inflicted by it spread well beyond the borders of those two countries.[55] This is not unique to NotPetya—many pieces of malware that have been designed for particular cyberattacks, such as the Stuxnet worm used to compromise Iranian nuclear enrichment tubes,[56] but spread far beyond their specific targets and infected computers belonging to victims who were in no way involved in the central conflict that motivated the attack.[57]

The disagreement among courts about the meaning of war continued in the years following the contradictory *Stankus* and *Rosenau* rulings. In 1945, the year after the *Rosenau* decision, the Supreme Court of Hawaii came to a similar decision as the Idaho court, ruling in favor of Gladys Ching Pang, who sued Sun Life Assurance Co. of Canada ("Sun Life") for refusing to pay out the life insurance policy of her husband, Tuck Lee Pang, a Honolulu Fire Department employee who died at Pearl Harbor.[58]

> On December 7, 1941, we not only were maintaining diplomatic relations with Japan but a special Japanese envoy was then in Washington ostensibly for the purpose of patching up the strained relations then existing between his country and ours, and not until December 8, 1941, did the political department of our Government or the Japanese Government do any act of which judicial notice can be taken creating "a state of war" between the two countries.[59]

The Supreme Court of Hawaii concluded that the Pearl Harbor attack did not fall within the war exclusion in Pang's life insurance policy and Sun Life was therefore required to pay his wife.[60]

The following year, in 1946, the Tenth Circuit Court of Appeals came to the opposite conclusion, following the model of the Supreme Court of Massachusetts in *Stankus*, by reversing a judgment for the beneficiaries of the life insurance policy belonging to Captain Mervyn S. Bennion, a naval officer who died at Pearl Harbor on the Battleship West Virginia.[61] Bennion's life insurance policy, also issued by New York Life Insurance,

---

[55] Satariano & Perlroth, *supra* note 14.

[56] Abraham & Schwarcz, *supra* note 11, at 13.

[57] CITI GPS, *supra* note 3, at 15.

[58] Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208, 208–09 (1945).

[59] *Id.* at 215–16.

[60] *Id.* at 222.

[61] N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260, 261, 265–66 (10th Cir. 1946).

contained exactly the same exception as Stankus's—word-for-word—and the Tenth Circuit determined that the exception applied to "any type or kind of war in which the hazard of human life was involved," including Pearl Harbor.[62] This, too, is a rationale that has significant implications for cyberattacks given how rarely even the most significant and devastating of them threaten human lives. Indeed, the fact that existing cases of cyberattacks have so rarely led to the loss of lives has been used to argue that these incidents do not constitute acts of war and that "cyber war" itself is unlikely to occur.[63]

The difference between the outcomes in favor of the insurers in *Stankus* and *Bennion* and the rulings for the insurance beneficiaries in *Rosenau* and *Pang* stems from a fundamental disagreement between the deciding courts about how narrowly and colloquially the language of an insurance policy should be interpreted—particularly, the term "war." The Supreme Courts of Idaho and Hawaii in *Rosenau* and *Pang*, respectively, were in favor of a very narrow legal interpretation of "war."[64] Meanwhile, the Tenth Circuit and Supreme Court of Massachusetts were instead focused on how people commonly understood war and the idea that, to many people, Pearl Harbor would *look* like an act of war, even if war between the United States and Japan had not yet been officially declared at the time of the attack.[65] The Tenth Circuit insisted that "[m]ankind goes no further in his definitive search [to understand what war is]- he does not stand on ceremony or wait for technical niceties."[66] In a similar vein, the Supreme Court of Massachusetts argued, "the words of an insurance policy . . . must be given their usual and ordinary meaning."[67] That "ordinary meaning," the Supreme Court of Massachusetts held, was determined by "ordinary people" and what they would consider to be war.[68] Justice Ronan explained, "[t]he term 'war' is not limited, restricted or modified by anything appearing in the policy. It refers to no particular type or kind of war, but applies in general to every situation that ordinary people would commonly regard as war."[69] While this

---

[62] *Id.* at 265.

[63] *See* THOMAS RID, CYBER WAR WILL NOT TAKE PLACE ch. 2 (2013).

[64] Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227, 230 (Idaho 1944); *Cladys Ching Pang*, 37 Haw. at 216–15.

[65] *Bennion*, 158 F.2d at 264; Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687, 688–89 (Mass. 1942).

[66] *Bennion*, 158 F.2d at 264.

[67] *Stankus*, 44 N.E.2d at 688.

[68] *Id.*

[69] *Id.*

"ordinary person" test may be common in insurance policy interpretation, it presents significant challenges when applied to emerging notions of cyber war, where there is little common consensus or understanding of when an online threat crosses the threshold of a warlike act even among experts, much less among ordinary people.

The evidence provided by the Massachusetts Court in *Stankus* relied heavily on the historical context of the moment when Stankus died—the hints that the United States was gearing up for military conflict in 1941, if not yet directly engaged in war.[70] Justice Ronan cited a September 11, 1941, address by President Roosevelt in which he declared, "[f]rom now on, if German or Italian vessels of war enter the waters the protection of which is necessary for American defense [sic], they do so at their own peril."[71] Ronan also cited the Lease-Lend Act in March 1941 as an indicator that the United States was already effectively engaging in war-related activities at the time of Stankus's death.[72]

> The President . . . had stated that German or Italian vessels of war entered these waters at their peril. The sinking by German or Italian submarines of ships belonging to a belligerent nation, or of ships of another nation convoying war materials and supplies to a belligerent nation, is the usual result of waging war by one nation against another, and the torpedoing of the Reuben James while convoying vessels engaged in such traffic was an act that arose out of the prosecution of such a war.[73]

It is striking that the President's statements carried so much weight with the Supreme Court of Massachusetts and hints at just how significant the public-facing language and political context of conflicts can be for determining when an event does or does not qualify for an insurance policy's war exception. After all, much stronger statements made by both the President and Congress following Pearl Harbor were quickly dismissed by the Idaho Supreme Court in the *Rosenau* case, which dealt with an incident that occurred much closer to the official declaration of war in the United

---

[70] *Id.* at 689.

[71] *Id.* at 688 (quoting *Fireside Chat 18: On the Greer Incident* (radio broadcast Sept. 11, 1941).

[72] *Id.* at 689. *See* H.R. 1776, 77th Cong. (1941).

[73] *Id.* (citations omitted).

States.[74] This uncertainty around the weight of public statements about the war-like nature of certain events also has important implications for cybersecurity incidents, particularly since terms like "cyber war" are thrown around freely for political purposes with relatively little consistency or clarity about what they actually mean.

The very different rulings in *Stankus* and *Bennion*, as compared to *Rosenau* and *Pang*, also make clear just how important the specific language of the actual exclusion written into an insurance policy can be. In *Rosenau*, for instance, the majority justified its decision to diverge from the rationale used to decide *Stankus* by stating that the war-related provisions in Stankus's life insurance coverage were "quite different" from those included in Rosenau's policy.[75] Unlike the *Stankus* and *Bennion* policies, which excluded deaths that resulted from "war or any act incident thereto,"[76] the *Rosenau* policy specifically excluded injuries "sustained while in military, naval, or air service of any country at war . . . ."[77] The Idaho Supreme Court focused particularly on the phrase "at war," arguing that it "very clearly" meant the exclusion only applied during a time when war had been legally declared.[78] Similarly, they distinguished the *Rosenau* case from an even earlier life insurance dispute brought after Alfred G. Vanderbilt died on May 7, 1915, aboard the British steamer Lusitania, when it was sunk by German submarines.[79] In that case—where the beneficiaries of Vanderbilt's life insurance lost against his insurer, Travelers' Insurance Co. ("Travelers")—the war exclusion had ruled out coverage for deaths "resulting, directly or indirectly, wholly or partly, from war [or riot]."[80] The absence of that crucial reference to a "time of war" differentiated the *Vanderbilt* policy from the *Rosenau* policy. Accordingly, the Idaho Supreme Court reasoned Travelers had more leeway to interpret the sinking of the British steamer Lusitania as an excluded act than Idaho Mutual had to interpret Pearl Harbor as occurring "in time of war."[81]

---

[74] Rosenau v. Idaho Mut. Benefit Ass'n, 145 P.2d 227, 229–30 (Idaho 1944).

[75] *Id.* at 231.

[76] *Stankus*, 44 N.E.2d at 687–88; N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260, 261 (10th Cir. 1946).

[77] *Rosenau*, 145 P.2d at 227.

[78] *Id.* at 231.

[79] *Id. See* Vanderbilt v. Travelers' Ins. Co., 184 N.Y.S. 54 (Sup. Ct. 1920), *aff'd*, 194 N.Y.S. 986 (App. Div. 1922), *aff'd*, 139 N.E. 715 (N.Y. 1923).

[80] *Rosenau*, 145 P.2d at 227 (quoting *Vanderbilt*, 184 N.Y.S. at 54).

[81] *Id.*

In other words, the majority in *Rosenau* did not hold that Pearl Harbor was any less an act of war than the torpedoing of the British steamer Lusitania or the U.S.S. Reuben James, but rather, they found that Idaho Mutual had crafted the language of their war exclusion more narrowly to apply only to deaths that occurred "in time of war." Indeed, one of the lessons for insurers following Pearl Harbor was that they should rewrite their war exclusions more broadly. Sun Life, for instance, changed the wording of its policies after Pearl Harbor. The life insurance policy in *Pang* issued by the company had excluded "death resulting from riot, insurrection, or war, or any act incident thereto," but shortly after Pearl Harbor the company modified that exclusion in new policies by inserting the words "whether declared or not" after the word "war."[82]

These early war exclusion disputes shaped the language of those exclusions for years to come, pushing insurers to broaden their descriptions of war to include undeclared war or warlike acts. This broadening of the terms of war exclusions to hedge what kinds of losses they could be applied to was not unique to life insurance; it spread into other insurance products, including property insurance. For instance, the policy Mondelez had purchased from Zurich at the time of the NotPetya ransomware attacks excluded property loss and damage "directly or indirectly caused by or resulting from . . . hostile or warlike action in time of peace or war . . . ."[83] This language had been deliberately crafted to apply to a much broader swath of circumstances than the narrower war exclusions that had appeared in the life insurance policies belonging to *Vanderbilt*, *Rosenau*, *Bennion*, *Stankus*, and *Pang* many decades earlier.

Almost a century before the NotPetya attacks, in June 1920, the Supreme Court of New York ruled in favor of Travelers in the *Vanderbilt* life insurance dispute.[84] The foundation of that ruling, disqualifying the claim on Vanderbilt's life insurance, was an assumption that any conflict between the governments of two countries constituted war, whether or not it had been officially and legally declared.[85] The Supreme Court of New York cited an even older maritime law case, decided in 1800, in which the United States Supreme Court had ruled that "every contention by force, between two nations, in external matters, under authority of their respective governments,

---

[82] Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208, 208, 211 (1945).

[83] Mondelez Complaint, *supra* note 2, at 4.

[84] *Vanderbilt*, 184 N.Y.S. at 56.

[85] *Id.*

is not only war, but public war."[86] Going by that logic, the Supreme Court of New York determined in the *Vanderbilt* life insurance case:

> The concessions of the parties that the Lusitania was sunk in accordance with instructions of a sovereign government, by the act of a vessel commanded by a commissioned officer of that sovereign government, being then operated by that said officer and its crew, all of whom were part of the naval forces of the said sovereign government, and that war was then being waged by and between Great Britain, the sovereign controlling the Lusitania, and Germany, the sovereign controlling the submarine vessel, control the conclusion which must be reached that the casualty resulted from war and that the consequences of the casualty come within the excepted portions of the policy.[87]

Twenty-six years later, the Tenth Circuit would use a similar rationale in deciding *Bennion*, where it determined that Pearl Harbor was an act of war.

> When one sovereign nation attacks another with premeditated and deliberate intent to wage war against it, and that nation resists the attacks with all the force at its command, we have war in the grim sense of reality. It is war in the only sense that men know and understand it.[88]

This, too, is a line of reasoning with significant implications for cyberattacks which are regularly directed by one sovereign government against another. Indeed, it was, in many ways, the crux of Zurich's argument that the NotPetya attacks were not covered under Mondelez's property insurance policy.[89] The ransomware attacks were not violent. It was not obvious that they looked like what an ordinary person might consider to be war. They did not occur at a time when the United States had officially declared war on the perpetrator, but that perpetrator was credibly believed

---

[86] *Id.* at 56 (quoting Bas v. Tingy, 4 U.S. (4 Dall.) 37, 40 (1800)).
[87] *Id.*
[88] N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260, 264 (10th Cir. 1946).
[89] *See* Mondelez Complaint, *supra* note 2, at 4.

by many to be Russia—a sovereign government.[90] Russia had not even formally declared war on Ukraine, the intended target of the NotPetya malware, though in 2014 the Ukrainian interim Prime Minister Arseniy Yatsenyuk referred to Russia's annexation of the Crimean Peninsula as "a declaration of war to my country."[91] However, while the malware targeted Ukrainian infrastructure, many of the victims of NotPetya, including Mondelez, were also private entities and organizations outside Ukraine,[92] so NotPetya was not exactly a "contention by force between two nations."[93] This was yet another way in which cyberattacks complicated traditional interpretations of war and war exclusions—the entanglement of public and private actors and the challenges of targeting cyberattacks so as not to cause widespread collateral damage under circumstances that insurers and earlier insurance disputes had not anticipated and for which insurers had not devised clear rules.

II. PAN AM FLIGHT 093 & EXPANSION OF WAR EXCLUSIONS TO TERRORISM

Pearl Harbor and the sinking of the British steamer Lusitania may not have been unambiguous acts of war, but they both certainly came much closer to situations "that ordinary people would commonly regard as war"[94] than NotPetya—a computer virus of ambiguous origin, at the time of its spread, that caused no direct casualties or violence and targeted mostly private companies.[95] More recent insurance disputes dealing with circumstances further removed from war than the British steamer Lusitania or Pearl Harbor, sheds some light on how war exclusions might apply to situations like NotPetya and other cyberattacks, as well as the role of these exclusions in property insurance policies, like the one Mondelez had purchased from Zurich. Ultimately, what these cases reveal is how much remains uncertain and unclear in the interpretation of insurance policy war

---

[90] *See* Satariano & Perloth, *supra* note 14 (noting the United States government blamed Russia in 2018); Brewster, *supra* note 13 (noting Ukraine blamed Russia in 2017).

[91] Marie-Louise Gumuchian, Ben Wedeman & Ian Lee, *Ukraine Mobilizes Troops After Russia's 'Declaration of War'*, CNN: WORLD (Mar. 3, 2014, 8:26 AM), https://www.cnn.com/2014/03/02/world/europe/ukraine-politics/index.html.

[92] Satariano & Perloth, *supra* note 14.

[93] Bas v. Tingy, 4 U.S. (4 Dall.) 37, 40 (1800).

[94] Stankus v. N.Y. Life Ins. Co., 44 N.E.2d 687, 688 (Mass. 1942).

[95] *See* CITI GPS, *supra* note 3, at 23–24.

exclusions, particularly when it comes to distinguishing between acts of war and acts of terrorism.

On September 6, 1970, Pan American World Airways Inc.'s ("Pam Am") Flight 093 was hijacked by two passengers, forty-five minutes after the Boeing 747 had departed from Amsterdam, heading to New York.[96] The two hijackers, armed with guns and grenades, ordered the pilot to fly to Beirut, Lebanon, and announced to the passengers and crew that they were working on behalf of the Popular Front for the Liberation of Palestine ("PFLP").[97] After the hijackers threatened to blow up the plane in mid-air, Lebanese officials permitted the flight to land in Beirut on the condition that it refuel and then leave.[98] On the ground in Lebanon, more PFLP members boarded the plane with explosives, and one—a demolition expert—stayed on the plane when it took off again, this time bound for Cairo.[99] Egyptian officials permitted the plane to land after the hijackers lit the fuses of the explosives while the plane was still in the air.[100] The hijackers informed the crew that they would have only eight minutes after the plane landed to evacuate everyone before the plane blew up, and the passengers were all successfully evacuated in Cairo.[101] The explosives detonated on schedule and the plane was subsequently destroyed.[102] Pan Am filed a claim with its insurers for the value of the aircraft, totaling $24,288,759.[103]

Pan Am had purchased comprehensive insurance coverage from several different insurers.[104] From Aetna Casualty and Surety Co. ("Aetna"), as well as other insurers, the airline had purchased all-risk insurance that covered one-third of the value of their fleet in the event of "all physical loss of or damage to the aircraft."[105] That policy excluded any losses or damage resulting from:

> 1. capture, seizure, arrest, restraint or detention or the consequences thereof or of any attempt thereat, or any

---

[96] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp 1098, 1100, 1104 (S.D.N.Y. 1973), *aff'd*, 505 F.2d 989 (2d Cir. 1974).

[97] *Id.* at 1100–01, 1114.

[98] *Id.* at 1114.

[99] *Id.*

[100] *Id.* at 1115.

[101] *Id.* at 1101, 1115.

[102] *Id.* at 1102.

[103] *Id.*

[104] *Id.*

[105] *Id.*

> taking of the property insured or damage to or destruction thereof by any Government or governmental authority or agent (whether secret or otherwise) or by any military, naval or usurped power, whether any of the foregoing be done by way of requisition or otherwise and whether in time of peace or war and whether lawful or unlawful . . . [hereinafter "Clause 1"];
> 2. war, invasion, civil war, revolution, rebellion, insurrection or warlike operations, whether there be a declaration of war or not [hereinafter "Clause 2"];
> 3. strikes, riots, civil commotion [hereinafter "Clause 3"].[106]

In order to ensure they would still be covered in the event of these excluded circumstances, Pan Am also purchased war risk insurance from Lloyd's, which had an upper limit of $14,226,290.47 in coverage and covered the three clauses of excluded risks in the all-risks policy, verbatim.[107] Since American underwriters did not offer war risk coverage, Pan Am obtained the rest of its war risk coverage, beyond what Lloyd's was willing to insure, from the United States government for an additional $9,763,709.53 of coverage that only applied to damage caused by the perils in the Clause 1 and Clause 2 of the Aetna policy exclusions.[108] This coverage was issued by United States Secretary of Commerce as authorized under the Federal Aviation Act of 1958, which allowed the government to provide insurance for risks that are excluded from commercial policies under "free of capture and seizure" clauses, like the Clause 1 and Clause 2 in Pan Am's all-risk policies exclusions.[109] Because the United States government was only authorized to cover risks excluded under "free of capture and seizure" clauses, this insurance could not apply to the Clause 3 exclusions—strikes, riots, and civil commotions—in Pan Am's all-risk insurance. So, in July 1970, just a few months before the hijacking, Pan Am came to an agreement with Aetna and its other insurers to make an additional premium payment of $29,935 in order to delete the Clause 3, which had previously ruled out

---

[106] *Id.*

[107] *Id.* at 1103–04.

[108] *Id.* at 1103.

[109] Federal Aviation Act of 1958, Pub. L. No. 85-726, §1301, 72 Stat. 731, 800–01 (1958) (current version at 49 U.S.C.A. §40101).

coverage for "strikes, riots, [and] civil commotion" and cover damage caused by those risks up to $10,062,393.[110]

Unsurprisingly, all of the insurers claimed that the hijacking was a type of risk covered by someone else's policy, leading to an extended legal battle. Aetna and the other all-risk insurers argued in court that the hijacking fell under the exclusions of Clause 1 and Clause 2—the ones it had no responsibility to cover—because it was perpetrated by a "'taking . . . by [a] military . . . or usurped power'" and was an example of "'insurrection,' 'rebellion,' 'civil war' . . . 'warlike operations,' 'war,' 'riot' and 'civil commotion.'"[111] Lloyd's and the United States government argued that the hijacking did not fall under any of the exception clauses and was therefore entirely the responsibility of the all-risk insurers.[112] Pan Am itself took this position as well, arguing that the hijacking was not an excluded risk; but further argued that, if the hijacking was an excluded risk, then it fell under the Clause 3 exclusion as a "riot" or "civil commotion."[113] Perhaps not coincidentally, these were the two interpretations—that the hijacking was not excluded or that it was an excluded Clause 3 peril—that would lead to the largest payouts for the company given the complicated coverage situation.[114]

New York District Judge Marvin Frankel ruled in 1973 that the Pan Am hijacking did not fall under any of the exclusion clauses, in a decision that discussed the political circumstances surrounding the Middle East and the PFLP at some length.[115] Aetna had argued that "the Arab-Israeli Conflict was the efficient cause of the hijacking operation" and that the hijacking should therefore be considered a war risk.[116] They also noted the hijackers' attempt to use the plane loudspeaker system to read a handwritten note to the passengers explaining that they were hijacking the plane "because the government of America helps Israel daily. The government of America gives Israel fantom airoplanes [sic] which attack our camps and burn our village."[117] Aetna argued that because the "seizure and destruction of the aircraft were announced by the group as a blow and as retaliation against the

---

[110] *Pan Am. World Airways, Inc.*, 368 F. Supp at 1102–03.

[111] *Id.* at 1117.

[112] *Id.* at 1103–04.

[113] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 996 (2d Cir. 1974).

[114] *Id.* at 1022.

[115] *Pan Am. World Airways, Inc.*, 368 F. Supp. at 1139.

[116] *Id.* at 1123.

[117] *Id.* at 1115.

United States. . . . [T]hese facts alone would be sufficient to place the loss under the broadly drawn war risk language."[118] Frankel rejected these arguments for relying on an overbroad definition of war; finding error in Aetna's justification for why the hijacking of the Pan Am plane qualified for the war risk exclusion because it "would apply equally to the bombing of stores in Europe, by children or adults, the killing of Olympic athletes, the killing of an American military attaché in Amman . . . or other individual acts of organization-sponsored violence in the United States or any other place."[119] Nor did he find that the larger Arab-Israeli conflict was to blame for the hijacking, or could be said to have "proximately caused" the incident.[120]

Several courts' rulings on computer fraud insurance cases in later years would focus on the question of whether a computer had directly or immediately caused an act of fraud, determining in many of those cases that the computer-based stages were too far removed from the actual theft for it to be considered an act of computer fraud.[121] Similarly, Frankel felt there was too much distance—both literally and metaphorically—between the conflict in the Middle East and the Pan Am hijacking for the latter to be viewed as an act of war, or even a direct consequence of war. Specifically, Frankel found "[i]t would take a most unusual and explicit contract to make the self-determined depredations of a terrorist group, thousands of miles from the area of the '[Arab-Israeli] Conflict,' acts of 'war' for insurance purposes."[122] And Aetna had not, in Frankel's view, authored a sufficiently explicit (or unusual) contract for this purpose.[123] In fact, Frankel noted that,

---

[118] *Id.* at 1123.

[119] *Id.*

[120] *Id.*

[121] *Compare* Brightpoint, Inc. v. Zurich Am. Ins. Co., No. 1:04-CV-2085, 2006 WL 693377 (S.D. Ind. Mar. 10, 2006) (reasoning that the fax of unauthorized checks and bank guarantees in payment for goods–here phone cards–did not meet Zurich policy's Computer Fraud requirement that the insured's loss be directly related to the use of a computer), *and* Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332, 333 (9th Cir. 2016) (affirming the district court's decision that the Computer Fraud provision "does not cover authorized or valid electronic transactions . . . even though they are, or may be, associated with a fraudulent scheme."), *with* Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 462–63 (6th Cir. 2018) (finding that the plaintiff's loss in this case was "directly caused" by the computer fraud when the plaintiff's employees conducted a series of actions, all induced by a fraudulent email).

[122] *Pan Am. World Airways, Inc.*, 368 F. Supp. at 1123.

[123] *Id.*

as in the case of the Pearl Harbor disputes, Aetna and the other all-risk insurers had changed the language of their exclusion clauses to respond to the hijacking, adopting "new exclusion clauses applying in adequate and unambiguous terms to operations like the PFLP hijackings."[124] In doing so, Frankel noted, they seemed to concede that "the former clauses lacked the clarity necessary to vindicate" their position in the Pan Am case that the previous language already unambiguously applied to hijackings.[125]

In 1974, the Second Circuit Court of Appeals upheld Frankel's ruling in finding that "war refers to and includes only hostilities carried on by entities that constitute governments at least de facto in character," and that the hijacking could not be considered a "'warlike operation' because that term does not include the inflicting of damage on the civilian property of non-belligerents by political groups far from the site of warfare . . . ."[126] While NotPetya is believed to have been developed and distributed by a government, there are echoes of what happened to Mondelez in this description of the Flight 093 hijacking. After all, Mondelez, and several other victims of the NotPetya malware, were caught up in the conflict between Russia and Ukraine despite being civilian victims located far from the Crimean Peninsula. Physical proximity to conflict is a more complicated and problematic consideration in cyberattacks than physical ones, since malware can so easily and quickly spread across geographic distance.[127] However, it is notable that this geographic distance from conflict was so central to the *Pan Am* ruling given how far-flung victims of cyberattacks often are from each other and the intended target of those attacks. This lack of geographic containment also contributes to the potential for even more highly correlated risks resulting from these incidents, causing even greater challenges for insurers.[128]

In the *Pan Am* case, the insurers tried to get around the fact that the PFLP was not a government by arguing that it was a "military . . . or usurped power" in Jordan and therefore still covered under the exceptions listed in Clause 1.[129] But the Second Circuit held "in order to constitute a military or usurped power the power must be at least that of a de facto government. On

---

[124] *Id.* at 1120.

[125] *Id.*

[126] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 997, 1012 (2d Cir. 1974).

[127] *See* CITI GPS, *supra* note 3, at 14, 83.

[128] Abraham & Schwarcz, *supra* note 11, at 50–52.

[129] *Pan Am. World Airways, Inc.*, 368 F. Supp. at 1129.

the facts of this case, the PFLP was not a de facto government in the sky over London when the 747 was taken."[130] Going clause by clause, the Second Circuit went on to eliminate each possible category of exception that the incident might have fallen under. The hijacking could not be considered a "warlike act" because "[t]he hijackers did not wear insignia. They did not openly carry arms. Their acts had criminal rather than military overtones. They were the agents of a radical political group, rather than a sovereign government."[131] It was not an "insurrection" because "the PFLP did not intend to overthrow King Hussein when it hijacked the Pan American 747."[132] It was not a "civil commotion" because "[f]or there to be a civil commotion, the agents causing the disorder must gather together and cause a disturbance and tumult."[133] It was not a "riot" because "the hijacking was accomplished by only two persons."[134]

If Aetna and Pan Am's other property insurers had intended for their policies to exclude hijackings then they should have used clearer, more specific language, the Second Circuit ruled.[135] In this regard, the Second Circuit suggested, the history of property insurance and its roots in early marine policies had not served the insurers well. The Second Circuit, in agreement with the District Court, dismissed the language of the Pan Am policy exclusions as being based on "ancient marine insurance terms selected by the all risk insurers simply do not describe a violent and senseless intercontinental hijacking carried out by an isolated band of political terrorists."[136]

III. HOLIDAY INN AND CIVIL COMMOTIONS

The *Pan Am* ruling that terrorist acts were not excluded from property insurance policies under war exclusions was highly influential in later legal disputes about what did or did not constitute an act of war under property insurance policies. In 1974, the same year that the Second Circuit issued its decision in the *Pan Am* case, a twenty-six floor Holiday Inn hotel

---

[130] *Pan Am. World Airways, Inc.*, 505 F.2d at 1009.

[131] *Id.* at 1015.

[132] *Id.* at 1018–19.

[133] *Id.* at 1020.

[134] *Id.* at 1021.

[135] *Id.* at 1009 ("[T]he all risk insurers were quite capable of resolving known ambiguities in concrete terms descriptive of today's events.").

[136] *Id.* at 998.

opened in Beirut, Lebanon.[137] In October 1975, conflict broke out in the neighborhood in West Beirut where the hotel was located between the Muslim Nasserist political party (called the "Mourabitoun") and the Christian right-wing party (called the "Phalange").[138] As the fighting continued in late 1975, members of the Phalangist militia occupied the Holiday Inn and the conflict caused considerable damage to the building—windows were shot out, fifteen rooms were damaged by fire, and another thirty-five had burned curtains and broken glass—forcing Holiday Inn to close the hotel to guests in November 1975.[139]

On "Black Saturday," December 6, 1975, the fighting in Beirut escalated significantly and the Holiday Inn became a focal point for the combatants.[140] All of the remaining staff were evacuated as the Phalangists claimed the hotel for themselves, and the building changed hands between the two sides several times over the course of the next few months as the fighting continued.[141] George McMurtrie Godley, who was serving as the American ambassador to Lebanon at the time, described the scene around the hotel:

> [You had] Christians occupying Holiday Inn. You had Moslems wanting to take it. Holiday Inn was right, you might say, on the borderline between the predominantly Christian areas and the predominantly Moslem areas. There you had rather well-organized military factions where men were holding an area and other men were attacking it.[142]

Holiday Inn had insured its foreign properties through Aetna under an all-risk policy similar to the one that covered Pan Am's fleet that provided coverage for "all risks . . . of direct physical loss or damage . . . from any external cause except as hereinafter provided."[143] Unlike Pan Am's policy, the Holiday Inn policy specifically included damage "directly caused by persons taking part in riots or civil commotion or by strikers or locked-out workers or by persons of malicious intent acting in behalf of or in connection

---

[137] Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp. 1460, 1467 (S.D.N.Y. 1983).

[138] *Id.* at 1468.

[139] *Id.* at 1469–70.

[140] *Id.* at 1470–71.

[141] *Id.* at 1471.

[142] *Id.* at 1479 n.73.

[143] *Id.* at 1463.

with any political organization . . . ."[144] In fact, Holiday Inn had agreed to higher premiums so that Aetna would include civil commotion coverage for their Beirut property.[145] But, the Holiday Inn policy still excluded any losses or damage caused "directly or indirectly, proximately or remotely . . . [by] [w]ar, invasion, act of foreign enemy, hostilities or warlike operations (whether war be declared or not), civil war, mutiny, insurrection, revolution, conspiracy, military or usurped power."[146] Unsurprisingly, when Holiday Inn filed a claim for nearly $11 million to cover the damage to their Beirut hotel, Aetna contended that the conflict between the Mourabitoun and the Phalangists had been a civil war or insurrection, and insurrection was therefore excluded from Holiday Inn's coverage.[147] Holiday Inn—like Pan Am—sued Aetna, insisting that the conflict was instead a form of "civil commotion" and therefore covered according to the terms for which it had specifically negotiated and paid extra.[148]

District Judge Charles S. Haight Jr., who decided *Holiday Inn* in 1983 in favor of the hotel chain, relied heavily on the *Pan Am* precedent in his ruling. Although Aetna had called various journalists to testify that the events in Beirut were widely regarded as a civil war, Haight rejected the testimony in favor of the assertion made by the Second Circuit in *Pan Am* that, "'the specific purpose of overthrowing the constituted government and seizing its powers' is a necessary element of both 'insurrection' and 'civil war.'"[149] Based on that definition, Haight found the events in Beirut could not be considered an insurrection because "the Mourabitoun, in seeking to dislodge the Phalange from the Holiday Inn, were not acting for the specific purpose of overthrowing the Lebanese government. They did not proclaim a casting off of allegiance to that government; they did not proclaim or seek to establish a government of their own."[150] It was not a civil war, according to Haight, because none of "the factions involved in any way with the damage to the Holiday Inn embraced partition of Lebanon as a specific objective."[151] Instead, Haight ruled:

---

[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] *Id.* at 1497 (quoting Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp 1098, 1124 (S.D.N.Y. 1973), *aff'd*, 505 F.2d 989 (2d Cir. 1974)).
[150] *Id.*
[151] *Id.* at 1498.

> The Holiday Inn was damaged by a series of factional "civil commotions," of increasing violence. The Lebanese government could not deal effectively with these commotions. The country came close to anarchy. But the constitutional government existed throughout; the requisite intent to overthrow it has not been proved to the exclusion of other interpretations; and there was no "war" in Lebanon between sovereign or quasi-sovereign states.[152]

Thanks to its foresight in negotiating special "civil commotion" coverage for an additional premium, Holiday Inn was therefore covered under its Aetna property insurance policy, and Aetna was ordered by the court to pay the claim.[153]

"Journalists and politicians invariably referred to these events in Lebanon as a 'civil war.' They do so today," Haight wrote towards the end of his ruling.[154] He went on to explain that regardless of how people commonly used those terms, his job was "to give the words at issue their insurance meaning . . . ."[155] Haight's willingness to dismiss the terms that people commonly used to describe the conflict is striking, as is his insistence that terms like "civil war" and "insurrection" could—and did—have a specific "insurance meaning," which is quite different from how they might be used and understood by the general public. Following Pearl Harbor, courts insisted that any event that looked to an ordinary person like war, should be considered as such for insurance purposes.[156] However, Haight (following in the footsteps of Frankel and the Second Circuit) was advocating for very narrow interpretations of the war exceptions written into property insurance policies.[157] This approach was in line with interpreting ambiguities in the coverage in favor of the policyholder, rather than the insurer.[158] In *Stankus*, the Massachusetts Supreme Court advocated for interpreting war under its

---

[152] *Id.* at 1503.

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *See* Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1157 (9th Cir. 2019) (holding that the lower court's application of the plain and ordinary meaning of 'war' was incorrect and instead affirming that for purposes of insurance, a special meaning should be applied).

[157] *Holiday Inns*, 571 F. Supp at 1464.

[158] *Id.*

"ordinary meaning,"[159] but Haight had no interest in the ordinary meaning of all-risk policy exclusions; he cared only about their insurance meaning.[160]

The idea that war has a very particular meaning and definition in the context of insurance contracts continued to gain traction in courts following the *Pan Am* and *Holiday Inn* rulings. In 2019, the Ninth Circuit Court of Appeals reversed a ruling in favor of the insurer, and an entire section of the opinion authored by Judge A. Wallace Tashima was captioned: "[*t*]*he special meaning of 'war' in the insurance context*."[161] The case was brought by Universal Cable Productions ("Universal"), which had been filming a television series called "Dig" in Jerusalem during the summer of 2014 when Hamas launched rockets at Israeli targets from Gaza, forcing the studio to shut down production and move filming to a new location.[162] Universal filed a claim with its insurer, Atlantic Specialty Insurance Co. ("Atlantic"), under their television production insurance policy to cover the costs of interrupting and moving production.[163] Atlantic denied the claim citing the four war exclusions in Universal's policy, which excluded coverage for losses caused by: (1) "[w]ar, including undeclared or civil war"; (2) "[w]arlike action by a military force;" (3) "[i]nsurrection, rebellion, [and] revolution;" and (4) "[a]ny weapon of war including atomic fission or radioactive force, whether in time of peace or war."[164]

In 2017, a district court in California concluded that Atlantic was correct in its assessment, and the Hamas attacks fell under the first two exclusion categories of war and warlike action because "[s]uch a conflict easily would be considered a 'war' by a layperson."[165] The district court based its analysis on California state law which dictated that the terms of an insurance policy must be "understood in their ordinary and popular sense, rather than according to their strict legal meaning . . . ."[166] The Ninth Circuit reversed the district court's decision, noting that, in fact, California law actually made an exception to its "ordinary and popular" rule on the interpretation of insurance policies if "a special meaning is given to them by

---

[159] Stankus v. N.Y Life Ins. Co., 44 N.E.2d 687, 688 (Mass. 1942).

[160] *Holiday Inns*, 571 F. Supp at 1503.

[161] *Universal Cable Prods., LLC*, 929 F.3d at 1154.

[162] *Id.* at 1146.

[163] *Id.* at 1146–47.

[164] *Id.* at 1149.

[165] Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 278 F. Supp. 3d 1165, 1173–74 (C.D. Cal. 2017), *rev'd in part*, *vacated in part*, 929 F.3d 1143 (9th Cir. 2019).

[166] *Id.* at 1172–73 (quoting CAL. CIV. CODE § 1644 (West 1872).

usage . . . ."[167] Citing both *Pan Am* and *Holiday Inn*, the Ninth Circuit determined that this exception applied to war on the grounds that "in the insurance context, the term 'war' has a special meaning that requires the existence of hostilities between de jure or de facto governments."[168] Since Hamas was not, in the Ninth Circuit's view, a de jure or de facto sovereign, its "conduct in the summer of 2014 cannot be defined as 'war' for the purposes of interpreting this policy."[169] Nor could the firing of those rockets be considered a warlike action, the Ninth Circuit ruled, because such a determination would conflate war with terrorism.[170] Tashima noted in the ruling that Hamas launched unguided missiles that were "likely used to injure and kill civilians because of their indiscriminate nature."[171] Therefore Tashima concluded, "Hamas' conduct consisted of intentional violence against civilians—conduct which is far closer to acts of terror than 'warlike action by a military force.'"[172]

A very narrow and particular meaning of war in the context of insurance policies, as well as a sharp distinction between warlike acts and terrorism, emerged from *Pan Am* and the cases that followed it like *Holiday Inn* and *Universal*. Both of those legacies—the narrow definition of war and the separation from terrorism—have significant implications for cybersecurity incidents like NotPetya, that appear to originate from government actors but that affect civilians.[173] Attribution of cyberattacks can be a slow and tricky endeavor,[174] but at least in the case of NotPetya, that process seemed to point unequivocally to the Russian government as the responsible party.[175] Moreover, the distribution of NotPetya in 2017 occurred in the midst of ongoing hostilities and armed conflict between two

---

[167] *Universal Cable Prods., LLC*, 929 F.3d at 1153 (quoting CAL. CIV. CODE § 1644 (West 1872).

[168] *Id.* at 1154.

[169] *Id.* at 1159.

[170] *Id.* at 1160.

[171] *Id.* at 1161.

[172] *Id.*

[173] *See* Satariano & Perloth, *supra* note 14.

[174] Ellen Nakashima, *Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[175] *Id.*

governments: Ukraine and Russia.[176] In this sense, an attack like NotPetya might seem to come closer to meeting the criteria for the insurance definition of war as "hostilities between de jure or de facto governments"[177] than an attack launched by a non-sovereign group like Hamas, Mourabitoun, or PFLP.[178]

On the other hand, while the perpetrator of NotPetya may have been a government actor, the victims were largely civilian and only those that were clearly elements of Ukraine's critical infrastructure—including Ukrainian power companies, transportation organizations, and banks—were clearly the intended targets due to their close ties to the ongoing Russia-Ukraine conflict.[179] Many other firms, both Ukrainian and non-Ukrainian, were affected indiscriminately by the malware, including Mondelez, and in those cases, Russia's use of a far-reaching, untargeted ransomware program suggests something closer to the Ninth Circuit's definition of terrorism as "intentional violence against civilians by political groups."[180] Perhaps most important, for all the extensive damage NotPetya caused, it was not a violent attack.[181] Unlike almost every other incident that has raised legal disputes on the meaning of war exclusions in insurance—the sinking of the British steamer Lusitania, the attack on Pearl Harbor to the hijacking of Pan Am Flight 093, and the attacks on Israel by Hamas—NotPetya did not directly put anyone's life in danger.[182] To call a piece of computer code, no matter how destructive, an act of war that resulted in no physical destruction or loss of lives would be to go against most people's common conceptions of what resembles war. In 2014, following the breach of Sony Pictures by the North Korean government, President Obama referred to the breach as "an act of cyber-vandalism that was very costly, very expensive" during an interview

---

[176] Sam Jones, *Finger Points at Russian State Over Petya Hack Attack*, FIN. TIMES (June 30, 2017), https://www.ft.com/content/f300ad84-5d9d-11e7-b553-e2df1b0c3220.

[177] *Universal Cable Prods., LLC*, 929 F.3d at 1154.

[178] *Id.* at 1147; Holiday Inns Inc. v. Aetna Ins. Co, 571 F. Supp. 1460, 1465 (S.D.N.Y. 1983); Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1013 (2d Cir. 1974).

[179] Andy Greenberg, *Petya Ransomware Epidemic May Be Spillover from Cyberwar*, WIRED (June 28, 2017, 1:02 PM), https://www.wired.com/story/petya-ransomware-ukraine.

[180] *Universal Cable Prods., LLC*, 929 F.3d at 1160.

[181] Greenberg, *supra* note 1 (estimating that damages stemming from the NotPetya attack totaled roughly $10 billion).

[182] Mondelez Complaint, *supra* note 2, at 2–3.

on CNN but said, explicitly, "I don't think it was an act of war."[183] NotPetya exhibited more elements of warlike activity than the Sony Pictures breach, including more immediate armed conflict between the central two nations involved, and targeting of critical infrastructure. But, for most of its non-critical infrastructure victims, NotPeya fundamentally shut down computers and deleted data (much like the Sony Pictures breach) rather than causing physical damages, [184] suggesting it still retained many more elements of an act of cyber-sabotage than a violent or warlike act. The key exception to this is the critical infrastructure targets of NotPetya, including the Ukrainian power grid—which resulted in some clear kinetic consequences[185]—raising the question of whether all victims and consequences of NotPetya should be lumped together for the purposes of classification, or whether the attacks on Mondelez might be categorized differently from those on Ukraine's power infrastructure, despite being executed by the same lines of code.

IV. MONDELEZ, NOTPETYA, AND THE MEANING OF CYBER WAR

When Mondelez was hit by the NotPetya ransomware in 2017, it had a comprehensive property insurance policy from Zurich that appeared to be explicitly designed to cover any digital disruptions to the company's business.[186] Specifically, the policy covered expenses "incurred by the Insured during the period of interruption directly resulting from the failure of the Insured's electronic data processing equipment or media to operate."[187] Following the attack, Mondelez promptly filed a claim with Zurich and provided documentation of the malware and its impacts.[188] On June 1, 2018, Mondelez received a letter from Zurich denying the claim on

---

[183] Sean Sullivan, *Obama: North Korea Hack 'Cyber-Vandalism,' Not 'Act of War',* WASH. POST (Dec. 21, 2014), https://www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/.

[184] *See, e.g.,* Mondelez Complaint, *supra* note 2, at 2–3. *See also* Greenberg, *supra* note 179.

[185] *See* Satariano & Perloth, *supra* note 14 ("In just 24 hours, NotPetya wiped clean 10 percent of all computers in Ukraine, paralyzing networks at banks, gas stations, hospitals, airports, power companies and nearly every government agency, and shutting down the radiation monitors at the old Chernobyl nuclear power plant.").

[186] Mondelez Complaint, *supra* note 2, at 2.

[187] *Id.*

[188] *Id.* at 3.

the grounds that NotPetya was excluded from their policy based on Exclusion B.2(a):

> 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
> (iii) agent or authority of any party specified in i or ii above.[189]

The war exclusion in Mondelez's policy bore many of the marks of insurers' efforts to broaden the language of their exclusions in light of previous court losses. The reference to warlike actions "in time of peace or war" codified the lesson of the Rosenau family's life insurance dispute about Pearl Harbor.[190] In that case, the insurance exclusion phrasing about policyholders "engaged in military or naval service in time of war" had been the insurer's downfall,[191] so insurers like Zurich now made sure to clarify that the war exclusions also applied at times when war had not been officially declared. The use of the term "warlike" was also an attempt to broaden the boundaries of a strict definition of war, just as it had been when used in the insurance policies disputed in *Pan Am*, *Holiday Inn*, and *Universal*. Further, the inclusion of any "agents or authority" of governments or sovereign powers in the scope of whose actions could be considered warlike hinted at yet another way in which Zurich was aiming to broaden the exclusion.

In the life insurance disputes following Pearl Harbor, the central question for the courts to decide was whether one country's attack on another's military could be considered war even absent a formal, legal

---

[189] *Id.* at 4.
[190] Rosenau v. Idaho Mut. Ben. Ass'n, 145 P.2d 227 (Idaho 1944).
[191] *Id.* at 231–32.

declaration.[192] In the more recent property insurance disputes about war exceptions in *Pan Am*, *Holiday Inn*, and *Universal*, the disagreements hinged chiefly on whether those exclusions encompassed violence directed at civilians by groups that were not governments.[193] NotPetya combined elements of both of these issues. Like the attack on Pearl Harbor, NotPetya emerged in the midst of ongoing, escalating conflict between two countries (in this case, Russia and Ukraine), and it appeared to have been developed and launched by a sovereign government, though the attribution to Russia took some months and was strenuously denied by the Russian government.[194] However, as in the *Pan Am*, *Holiday Inn*, and *Universal* cases, NotPetya primarily affected civilian victims rather than military ones, and many of those targets—including Mondelez—were outside Ukraine and fairly far removed from the political conflict between the two governments.[195] And unlike *Pan Am*, *Holiday Inn*, and *Universal*, NotPetya caused no direct physical damage to the Mondelez's property.[196] However, that did not invalidate the insurance coverage since Mondelez's policy from Zurich explicitly included coverage for business interruptions and the associated losses that were caused by the failure of computers.[197] But it did make the incident seem, on the whole, slightly less "warlike" than an airplane hijacking or a missile attack.

The strongest evidence in favor of Zurich's assertion that NotPetya was a "hostile or warlike action" lay in the attack being attributed to the Russian government.[198] That process of attribution lasted months and took

---

[192] *Id.* (noting the war exclusion did not apply because "no act or recognition had taken place by any department of our government with regard to the existence of war, or warlike activities, at the time of the death of the insured.").

[193] Universal Cable Prods., LLC, v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1154 (9th Cir. 2019); Holiday Inns Inc. v. Aetna Ins. Co, 571 F. Supp. 1460 (S.D.N.Y. 1983); Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974).

[194] Denis Pinchuk, *Russia Denies British Allegations That Moscow Was Behind Cyber-Attack*, REUTERS (Feb. 15, 2018, 4:50 AM), https://www.reuters.com/article/us-britain-russia-cyber-kremlin/russia-denies-british-allegations-that-moscow-was-behind-cyber-attack-idUSKCN1FZ102.

[195] Mondelez Complaint, *supra* note 2, at 2. *See also* Greenberg, *supra* note 179 ("Hackers may instead have been continuing a long-running assault against Ukraine. But this time, the rest of the world feels their pain too.").

[196] Mondelez Complaint, *supra* note 2, at 2–3.

[197] *Id*. at 2.

[198] Jones, *supra* note 176.

place during the nearly year-long period between Mondelez's initial filing of an insurance claim and Zurich's denial of that claim.[199] Beginning immediately after the NotPetya attacks in June 2017, Ukrainian officials and cybersecurity researchers were quick to cast blame for the attack on Russia.[200] That same month, Roman Boyarchuk, who ran Ukraine's Center for Cyber Protection, told *Wired* that the attack was "likely state-sponsored" and that it was "difficult to imagine anyone else," besides Russia, who "would want to do this."[201] Ukrainian cybersecurity firm, Information Systems Security Partners, was also among the first to claim that the NotPetya code closely resembled previous Russian cyberattacks in its design and technical "fingerprints."[202] Later that month, United States cybersecurity company, FireEye, made a similar claim, when its head of global cyber intelligence, John Watters, told *The Financial Times*, "we are reasonably confident towards it being Russia" that was responsible for NotPetya, based on analysis of the targets, code, and malware infection vectors.[203] "The best you can get is high confidence," Watters said of the attribution effort, emphasizing that it was not definite Russia was behind the attack even though "there are a lot of things that point to Russia."[204]

On February 14, 2018, the UK National Cyber Security Centre published a statement saying the Russian military was "almost certainly responsible" for NotPetya.[205] The next day, February 15, 2018, the Australian Minister for Law Enforcement and Cyber Security, Angus Taylor, issued a similar statement that "the Australian Government has judged that Russian state sponsored actors were responsible" for NotPetya,[206] as did White House press secretary, Sarah Huckabee Sanders. Sanders' brief statement read, in its entirety:

---

[199] *Id.*

[200] Greenberg, *supra* note 179.

[201] *Id.*

[202] *Id.*

[203] Jones, *supra* note 176.

[204] *Id.*

[205] *Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack*, NAT'L CYBER SEC. CTR. (Feb. 14, 2018), https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

[206] Asha Barbaschow, *Australia Also Points Finger at Russia for NotPetya*, ZDNET (Feb. 15, 2018), https://www.zdnet.com/article/australia-also-points-finger-at-russia-for-notpetya/.

> In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.
>
> The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.[207]

Four more countries—Canada, Denmark, Lithuania, and Estonia—quickly followed suit, issuing official statements blaming Russia for the attack within the week in what Australia's Ambassador for Cyber Affairs, Tobias Feakin, later referred to as "the largest coordinated attribution of its kind to date."[208] A spokesman for the Russian government, Dmitry Peskov, denied the coordinated allegations and denounced them as "Russophobic."[209]

It is, of course, difficult to say definitively whether the Russian government was behind the NotPetya malware, but Zurich's case for claiming the incident was the act of a "government or sovereign power" is about as persuasive as it is possible for a cyberattack attribution to be.[210] The evidence pointing to Russia includes similarities between the NotPetya code and previous strains of malware attributed to Russia.[211] While most ransomware encrypts the contents of infected computers and then provides a way for victims to decrypt their files so long as they make a cryptocurrency ransom payment, NotPetya did not only encrypt the hard drives of computers it infected.[212] It also overwrote the master boot records of those computers, making it nearly impossible for the files to be restored.[213] Additionally, while NotPetya did appear to demand a (relatively small) ransom payment from victims of roughly $300 in bitcoin, the ransom demand was unusual in that

---

[207] WHITE HOUSE, Statement from the Press Sec'y (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

[208] Stilgherrian, *Blaming Russia for NotPetya was Coordinated Diplomatic Action*, ZDNET (Apr. 11, 2018), https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

[209] Pinchuk, *supra* note 194.

[210] Mondelez Complaint, *supra* note 2, at 4.

[211] Greenberg, *supra* note 179.

[212] Jones, *supra* note 176.

[213] *Id.*

it required victims to send confirmation of their payments to a particular, fixed email address.[214] That address was quickly blocked by the email service provider after the attack began—making it difficult for anyone to prove they had actually paid the demanded ransom according to the attackers' terms.[215]

The signs that the attackers did not actually aim to restore their victims' files and had no real interest in collecting ransom payments, hinted that the perpetrators were not financially motivated criminals, but instead had some other agenda.[216] That agenda was clarified somewhat by the fact that the perpetrators initially spread NotPetya by embedding it inside a software update from a Ukrainian accounting software company called MeDoc.[217] Because a Ukrainian firm was used as the initial conduit, most of the victims of NotPetya were Ukrainian. In fact, early estimates suggested that more than three-quarters of the affected organizations were based in Ukraine—though the malware quickly spread to other companies outside Ukraine, at least in part through their infected Ukrainian subsidiaries.[218] This focus on Ukraine aligned with earlier Russian cyberattacks focused on Ukrainian infrastructure, as well as the ongoing military conflict between the two countries dating from Russia's annexation of Crimea in February 2014—a conflict sometimes referred to as the "Russo-Ukrainian War."[219]

This political context—and even the language used to describe it—is relevant to Zurich's argument that NotPetya was a "warlike action."[220] In July 2019, six months after Mondelez filed its lawsuit against Zurich, the Ninth Circuit issued its *Universal* ruling stating, "in the insurance context, the term 'war' has a special meaning that requires the existence of hostilities between de jure or de facto governments."[221] The conflict between Russia and Ukraine certainly appeared to meet that bar of hostilities between governments, and the coordinated attribution of NotPetya to Russia by several countries in February 2018, three and a half months before Zurich denied the Mondelez claim, gave Zurich a strong basis for arguing that NotPetya had been perpetrated by a government party to those hostilities.

---

[214] *Id.*

[215] *Id.*

[216] Greenberg, *supra* note 179.

[217] Jones, *supra* note 176.

[218] *Id.*

[219] Joshua P. Mulford, *Non-State Actors in the Russo-Ukrainian War*, 15 CONNECTIONS: Q.J. 89, 89–106 (2016).

[220] Mondelez Complaint, *supra* note 2, at 4.

[221] Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1154 (9th Cir. 2019).

What was less clear was whether NotPetya itself—or any computer-based attack, for that matter—could legitimately be considered "warlike."

Mondelez thought not. In its lawsuit against Zurich, the company referred to "Zurich's invocation of a 'hostile or warlike action' exclusion to deny coverage for malicious 'cyber' incidents" as "unprecedented."[222] Indeed, no previous legal conflicts that centered on interpretation of insurance war exclusions had dealt with cyberattacks, nor was there any reason to believe that the exclusions had been crafted to apply to computer-based attacks. This supported Mondelez's claim that "the purported application of this type of exclusion to anything other than conventional armed conflict or hostilities was unprecedented."[223] But just because Zurich's interpretation of the war exclusion was unprecedented did not necessarily mean it was wrong. In fact, much of Mondelez's argument seemed to lie in simply asserting that "incursions of malicious code or instruction into MDLZ's [Mondelez's] computers did not constitute 'hostile or warlike action,' as required by Exclusion B.2(a)."[224] In framing its argument this way, Mondelez implied that malware directed at a private company, that plays no role in a country's critical infrastructure, cannot constitute "hostile or warlike action" rather than asserting that every victim or impact of NotPetya should necessarily be considered un-warlike.[225]

By the time Mondelez filed its lawsuit, there was already a growing trend of nations and international organizations recognizing that cyberattacks were rapidly becoming an integral part of warfare and that "incursions into computers" had the potential to cause serious damage, on par with the destruction of kinetic attacks. For instance, in June 2016, a year before NotPetya, NATO Secretary-General Jens Stoltenberg told the German newspaper, *Bild*, that the alliance had classified cyberspace as an "official domain of warfare" and confirmed that a sufficiently severe cyberattack on any of its members would be considered an act of war, triggering a military response.[226] At the time, Stoltenberg did not point to any specific examples of known cyberattacks that had reached that level, but

---

[222] Mondelez Complaint, *supra* note 2, at 4.

[223] *Id.*

[224] *Id.* at 4–5.

[225] *Id.*

[226] Andrea Shalal, *Massive Cyber Attack Could Trigger NATO Response: Stoltenberg*, REUTERS (June 15, 2016, 5:38 PM), https://www.reuters.com/article/us-cyber-nato/massive-cyber-attack-could-trigger-nato-response-stoltenberg-idUSKCN0Z12NE.

some experts later indicated that the use of cyber capabilities by Russia against Ukraine was a prime example of what such warlike actions in cyberspace might look like.[227]

On March 29, 2017, just a few months before NotPetya hit Mondelez, Center for Strategic and International Studies adviser Olga Oliker testified before the Senate Armed Services Subcommittee on Emerging Threats and Capabilities that if an earlier attack on the Ukrainian electric grid had been perpetrated by Russia, then it was "an example of precisely the type of cyber operation that could be seen as warfare."[228] But whether the collateral damage of that operation and the malware designed for it, including the impacts of NotPetya on companies like Mondelez, could also be seen as warfare was less clear from Oliker's testimony.[229] Looking back at earlier lawsuits over the application of insurance war exclusions, many of which prominently feature public statements from political figures, journalists, and experts about whether the relevant events were akin to war, it is not hard to imagine Zurich building its case on statements like this one by Oliker. For instance, *Wired* reporter Andy Greenberg, who did extensive reporting on NotPetya and in 2020 published a book about it titled *Sandworm*, wrote in one of his widely read articles about the attack, "[t]he release of NotPetya was an act of cyberwar by almost any definition."[230]

Some courts—for instance, the Massachusetts Supreme Court in *Stankus* looking at President Roosevelt's address—have been swayed by public statements and popular coverage of the events at issue in insurance cases.[231] But this is typically only the case for courts that believe that the meaning of war in an insurance context is the same as its common meaning in everyday parlance. The more recent trend of war exception cases, since the *Pan Am* ruling, has been to insist on a narrower, insurance-specific definition of war that operates independently of the language and terms used by the broader public. In the *Holiday Inn* ruling, for instance, the deciding judge was quite ready to dismiss the fact that "[j]ournalists and politicians invariably referred to these events in Lebanon as a 'civil war'" on the

---

[227] *See, e.g.*, Greenberg, *supra* note 1; *Russian Influence and Unconventional Warfare Operations in the 'Grey Zone:' Lessons from Ukraine*: *Statement before the S. Armed Servs. Comm., Subcomm. on Emerging Threats and Capabilities,* 115th Con. (2017) (statement by Dr. Olga Oliker, Senior Adviser & Dir, Russ. and Eurasia Program, Ctr. for Strategic & Int'l Stud.), https://www.armed-services.senate.gov/imo/media/doc/Oliker_03-29-17.pdf [hereinafter *Statement by Dr. Olga Oliker*].

[228] *Statement by Dr. Olga Oliker*, *supra* note 227, at 5.

[229] *Id.*

[230] Greenberg, *supra* note 1.

[231] Stankus v. N.Y Life Ins. Co., 44 N.E.2d 687, 688–89 (Mass. 1942).

grounds that it was irrelevant to determining whether the conflict was a civil war in the "insurance meaning" of the words.[232] It seems plausible that a court could similarly dismiss references to NotPetya as an act of cyber war as irrelevant to the question of whether the cyberattack qualified as warlike in an insurance context.

One insurance broker, Marsh & McLennan ("Marsh"), took a strong stand to this effect in August 2018, shortly after Zurich denied Mondelez's claim, but before Mondelez filed its lawsuit. In a short article titled *NotPetya Was Not Cyber 'War'*, Matthew McCabe, Marsh's assistant general counsel for cyber policy, made the case that NotPetya was not a warlike action and should therefore not be excluded from insurance coverage under war exceptions.[233] "For a cyber-attack to reach the level of warlike activity, its consequences must go beyond economic losses, even large ones," McCabe wrote.[234] Furthermore, he pointed out, "[t]he most prominent victims of NotPetya operated far from any field of conflict and worked at purely civilian tasks like delivering packages, producing pharmaceuticals, and making disinfectants and cookies."[235] As the representative of an insurance broker, an organization that assists customers purchase insurance policies, McCabe clearly had an interest in representing his clients' interests and persuading them that continuing to purchase these types of policies was worthwhile and not a waste of money. But even if his motives may have been influenced by his employer's business interests, McCabe's concluding call for greater clarity in war exclusions is an important one. "[I]f insurers are going to continue including the war exclusion on cyber insurance policies, the wording should be reformed to make clear the circumstances required to trigger it."[236]

Perhaps the strongest piece of Mondelez's argument is that the language of Exclusion B.2(a) is "vague and ambiguous" and that "Zurich's failure to modify that historical language to specifically address the extent to which it would apply to cyber incidents" means it "therefore must be

---

[232] Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp.1460, 1503 (S.D.N.Y. 1983).

[233] Thomas Reagan & Matthew McCabe, *NotPetya Was Not Cyber "War", in* MMC CYBER HANDBOOK 2019: PERSPECTIVES ON CYBER RISK IN THE DIGITAL ERA 18 (2019), https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2019/mar/OWY22801-076_Cyber-Handbook-2019-Digital.pdf.

[234] *Id.* at 18.

[235] *Id.*

[236] *Id.*

interpreted in favor of coverage."[237] The courts in *Pan Am*, *Holiday Inn*, and *Universal* ruled in favor of policyholders rather than their insurers in large part based on this rationale—that absent specific language excluding a certain scenario, courts were generally inclined to interpret the exclusions fairly narrowly.[238] On the other hand, in a certain light, NotPetya could be viewed as fitting even that narrow definition because, unlike the incidents in *Pan Am*, *Holiday Inn*, and *Universal*, the perpetrator appeared to be a sovereign government engaged in hostilities with another country. When the Second Circuit determined that the hijacking of Pan Am Flight 093 was not a warlike act, it based that decision largely on the fact that the hijackers' "acts had criminal rather than military overtones. They were the agents of a radical political group, rather than a sovereign government."[239] Similarly, the *Holiday Inn* ruling rested in part on the fact that "there was no 'war' in Lebanon between sovereign or quasi-sovereign states."[240] Neither of those rationales quite fit the NotPetya case, assuming one accepts the attribution of the attack to Russia and the extensive documentation that it was part of the conflict with Ukraine.

The *Universal* ruling offers perhaps the most support for Mondelez's contention that NotPetya was not a warlike action. In that case, the Ninth Circuit highlighted the "indiscriminate nature" of the unguided missiles used by Hamas as evidence that they were trying to injure and kill civilians, conduct that the court ruled was "far closer to acts of terror" than "warlike action."[241] NotPetya could also be viewed as an indiscriminate or unguided weapon, one that caused significant damage to civilian targets—including Mondelez. Indeed, Mondelez's distance from the Russia-Ukraine conflict could work in its favor. Just as the Second Circuit ruled that the Pan Am hijacking could not be considered a "warlike operation" because "that term does not include the inflicting of damage on the civilian property of non-belligerents by political groups far from the site of warfare,"[242] so, too, a court could conceivably determine that it was a stretch to deem "warlike" the

---

[237] Mondelez Complaint, *supra* note 2, at 16.

[238] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1022 (2d Cir. 1974); Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp.1460, 1503 (S.D.N.Y. 1983); Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co., 929 F.3d 1143, 1162 (9th Cir. 2019).

[239] *Pan Am. World Airways, Inc.*, 505 F.2d at 1015.

[240] *Holiday Inns Inc.*, 571 F. Supp. at 1503.

[241] *Universal Cable Prods., LLC*, 929 F.3d at 1161.

[242] *Pan Am. World Airways, Inc.,* 505 F.2d at 997.

inflicting of damage on the civilian property of a multinational food company headquartered in Chicago, Illinois, far from Russia and Ukraine.[243]

V. CRAFTING WAR EXCLUSIONS FOR CYBERATTACKS

One of the more fascinating elements of Mondelez's lawsuit is its description of Zurich's behavior in the aftermath of issuing its formal coverage denial letter on June 1, 2018.[244] According to Mondelez, soon after sending that letter, Zurich appeared to change its mind and told the firm that it would rescind the declination of coverage and resume adjustment of Mondelez's claim.[245] On July 18, 2018, Zurich sent Mondelez an email "formally rescind[ing]" its previous coverage denial and promising to resume work on the claim.[246] Then, in another email sent less than a week later on July 24, Zurich offered Mondelez a $10 million partial payment towards the company's insurance claim.[247] However, that payment never materialized—nor did Zurich ever appear to resume work on the claim.[248]

Mondelez, in its complaint against Zurich, is quick to assert that these prevarications on Zurich's part stemmed from the insurer's fears that denying Mondelez's claim might lead to bad publicity.[249] The July 2018 emails, promising a $10 million advance payment and a continued claim adjustment process, were aimed at convincing Mondelez "to refrain from filing immediate litigation," the company alleges in its lawsuit.[250] If that was in fact the intention of those emails, then they seem to have worked since Mondelez waited until January 2019 to file its lawsuit, more than six months after its initial claim was denied by Zurich because of the "explicit representations and promises from Zurich" made in the July 2018 emails.[251]

Zurich was hoping to prevent, or at the very least delay, a lawsuit, Mondelez contended, because the insurer feared the publicity surrounding such a suit would draw attention to all the ways that Zurich policies might not actually cover cyberattacks.[252] Mondelez goes so far as to claim in its

---

[243] Mondelez Complaint, *supra* note 2, at 5.
[244] *Id*.
[245] *Id.*
[246] *Id.*
[247] *Id.*
[248] *Id.* at 6.
[249] *Id.* at 5.
[250] *Id.*
[251] *Id.*
[252] *Id.* at 8.

lawsuit that Zurich feared the publicity would "adversely impact its dealings with actual and prospective policyholders who were considering the purchase or renewal of insurance coverage from Zurich."[253] Whether or not this was actually the line of reasoning behind the mixed signals Zurich sent Mondelez in the summer of 2018, it is clear that the insurer was undecided, or at the very least uncertain, about how to handle the NotPetya claim. For one thing, it was an extraordinarily expensive cyberattack—the United States government dubbed it "the most destructive and costly cyber-attack in history" in February 2018, and later reports estimated that the damages totaled roughly $10 billion.[254]

For Zurich, and other insurers, the issues raised by the Mondelez claim were much larger than just coverage for the losses borne by one company—they spoke to the question of who would bear the costs NotPetya inflicted on hundreds of companies across the world. For instance, pharmaceutical firm Merck estimated that it had suffered $870 million in damages from NotPetya, ranging from its 30,000 infected laptop and desktop computers to its inability to meet demand for the Gardasil 9 vaccine used to prevent HPV.[255] Merck, like Mondelez, had extensive insurance coverage for property damage and catastrophic risks—a total of $1.75 billion in coverage, in Merck's case, less a $150 million deductible.[256] But most of Merck's thirty insurers and reinsurers, like Zurich, denied the pharmaceutical company's claims citing war exclusions. Merck, like Mondelez, subsequently sued those insurers—a group that included several prominent cyber-insurance providers such as Allianz and AIG—for $1.3 billion under its property insurance policies.[257] Merck's arguments for why the war exclusions do not apply to NotPetya closely mirrored Mondelez's, and primarily center on the claim that those exclusions were never intended to address cybersecurity incidents or tailored to that purpose. Merck argued:

> The "war" and "terrorism" exclusions do not, on their face, apply to losses caused by network interruption events such

---

[253] *Id.* at 17.

[254] Andy Greenberg, *The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack in History',* WIRED (Feb. 15, 2018, 6:20 PM), https://www.wired.com/story/white-house-russia-notpetya-attribution.

[255] David Voreacos, Katherine Chiglinsky & Riley Griffin, *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, BLOOMBERG L. (Dec. 3, 2019, 12:01 AM), https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war.

[256] *Id.*

[257] *Id.*

> as NotPetya, . . . [t]hey do not mention cyber events, networks, computers, data, coding, or software; nor do they contain any other language suggesting an intention to exclude coverage for cyber events.[258]

In an opinion in the Merck case issued on December 6, 2021, Judge Thomas J. Walsh sided with Merck, ruling that the war exclusion in its property insurance did not apply to NotPetya because Merck's "reasonable understanding of this exclusion involved the use of armed forces, and all of the caselaw on the war exclusion supports this interpretation."[259] Walsh particularly called out the insurance companies for failing to update the language of the exclusion if they intended for it to cover state-sponsored cyberattacks, pointing out that "the language used in these policies has been virtually the same for many years."[260] He continued, "both parties to this contract are aware that cyber attacks of various forms, sometimes from private sources and sometimes from nation-states have become more common. Despite this, Insurers did nothing to change the language of the exemption to reasonably put this insured on notice that it intended to exclude cyber attacks. Certainly they had the ability to do so."[261] This portion of the ruling strongly suggests that insurers will now hasten to change those exceptions to more explicitly rule out coverage for large-scale cyberattacks—if they have not done so already.

Undoubtedly, property and other types of insurance policies dealing with cyber risks will contain exactly that sort of language in the future, due in no small part to NotPetya and the resulting, as-yet-unresolved disputes initiated by companies like Mondelez and Merck. On November 13, 2019, the Lloyd's Market Association introduced new cyber exclusions, the Property D&F Cyber Endorsement, or LMA5400, and the Property Cyber and Data Exclusion, LMA5401, both of which would exclude from coverage any losses resulting from malicious cyber acts as well as non-malicious cyber incidents resulting from errors or omissions in the operation of computer

---

[258] *Id.* (quoting Plaintiff's Requests to Produce Documents, Merck & Co. v. Ace Am. Ins. Co., No. UUN-L-2682 (N.J. Super. Ct. Law Div. Aug. 1, 2019)

[259] Merck & Co. v. Ace Am. Ins. Co., No. UUN-L-2682 at 8 (N.J. Super. Ct. Law Div. Dec. 6, 2021) (Bloomberg Law, Court Dockets).

[260] *Id.* at 10.

[261] *Id.* at 10–11.

systems or any outages or malfunctions of those systems.[262] NotPetya and the resulting claims activity did not just reshape the cyber exclusions in property policies, it also had a profound influence on the exclusions written into stand-alone cyber policies as well. In this case, however, insurers were more concerned about assuaging customers' concerns that war exclusions would prevent them from being able to exercise such policies. Kenneth Abraham and Daniel Schwarcz point out that construing war exclusions to apply broadly to cyberattacks initiated by nation states could lead to exclusion of many types of online threats that policyholders would expect to have covered by cyber-insurance policies.[263] They note that, "unlike in traditional insurance settings, it is often difficult or impossible for cyber insurers to identify and exclude from coverage the casual mechanisms of potentially catastrophic cyber risks without eviscerating coverage for ordinary cyberattacks that policyholders demand."[264]

In order to reassure policyholders that stand-alone cyber policies would still be useful in the wake of NotPetya claim denials, cyber-insurers began to explicitly include coverage for "cyberterrorism" in those products, without ever quite clarifying how cyberterrorism differed from warlike acts. For instance, Zurich's stand-alone cyber-insurance policy template, covering first- and third-party losses related to breaches, extortion, privacy incidents, and social engineering, included a "War or Civil Unrest" exclusion for costs incurred by:

> 1. war, including undeclared or civil war;
> 2. warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign, or other authority using military personnel or other agents; or
> 3. insurrection, rebellion, revolution, riot, usurped power, or action taken by governmental authority in hindering or defending against any of these.[265]

---

[262] Andrew Hill, *Cyber Risk Poses Ongoing Challenge for First-Party Property Damage Lines of Business,* WILLIS TOWERS WATSON (Jan. 28, 2020), https://www.willistowerswatson.com/en-US/Insights/2020/01/cyber-risk-poses-ongoing-challenge-for-first-party-property-damage-lines-of-business.

[263] Abraham & Schwarcz, *supra* note 11, at 37.

[264] *Id.*

[265] ZURICH CYBER INSURANCE POLICY U-SPR-200-A CW (09/18) 23 (2018) (on file with author).

However, perhaps in recognition of the concerns policyholders might have about this exclusion following the Merck and Mondelez claim denials, the Zurich policy explicitly stated that their war and civil unrest exclusion did not apply to "cyberterrorism."[266] The policy defined cyberterrorism separately as:

> [T]he use of information technology to execute attacks or threats against Your Network Security by any person or group, whether acting alone, or on behalf of, or in connection with, any individual, organization, or government, with the intention to:
>
> 1. cause harm;
> 2. intimidate any person or entity; or
> 3. cause destruction or harm to critical infrastructure or data, in furtherance of financial, social, ideological, religious, or political objectives.[267]

In a 2020 analysis of fifty-six cyber-insurance policies, Daniel Woods and Jessica Weinkle suggested that this emerging trend for cyber-insurance to affirmatively cover cyberterrorism had "weakened" the war exclusions in such policies.[268] But it was not clear from those broad definitions which category an attack like NotPetya would fall under, so the inclusion of cyberterrorism in their coverage did little to resolve the ambiguities and uncertainty faced by policyholders.

The rewriting of insurance policy exclusions is typical of the aftermath of significant legal controversies over denied claims tied to war. For example, Sun Life broadened its life insurance exception to apply to "war, whether declared or not" after Pearl Harbor,[269] and Aetna excluded hijackings following the explosion of Pan Am Flight 093.[270] Clearly, insurers need to do a better job of describing more clearly which computer-based threats are excluded from their coverage, but rephrasing the insurance exclusions that apply to cyber risks will be no small feat for insurers as the

---

[266] *Id.*

[267] *Id.* at 8.

[268] Daniel W. Woods & Jessica Weinkle, *Insurance Definitions of Cyber War,* 45 GENEVA PAPERS ON RISK & INS. 639, 639 (2020).

[269] Cladys Ching Pang v. Sun Life Assurance Co. of Can., 37 Haw. 208, 208, 211 (1945).

[270] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp 1098, 1120 (S.D.N.Y. 1973), *aff'd*, 505 F.2d 989 (2d Cir. 1974).

attempts to differentiate between cyber war and cyberterrorism already indicate. Defining clearer exclusions for cyberattacks will be challenging both because of the broad range of threats carriers have to consider, and because at the same time, they are trying to exclude certain threats. Many insurers are also aggressively developing and marketing cyber-insurance policies designed to cover other, closely related online threats.

One of the striking differences between the definitions of warlike actions and cyber terrorism in these cyber-insurance policies is that while the former relies primarily on attribution and being able to reliably identify whether or not a nation state, governmental authority, or military force is the perpetrator of an attack, the latter focuses instead on the impacts of the incident in question. Classifying cyberattacks according to the kind of damage they do to data or critical infrastructure has several advantages over trying to categorize them based on their perpetrators and broader political context. First, attribution remains a challenging and slow process for many cyberattacks, but the impacts of those incidents are often much clearer and less controversial in their immediate aftermath. So using those impacts as a means of determining whether a cyberattack is covered under an insurance policy has the potential to avoid disputes over attribution and instead focus on the less contentious fall-out of those attacks. Second, this approach could allow for the disaggregation of different victims impacted by the same malware or attack vector. Instead of considering NotPetya as a piece of malware, to be itself a warlike act because it was created by a particular entity, the code's impacts on different victims and targets could be evaluated separately, each in their own respective context. This would help address the challenge of narrowly targeting cyberattacks and the subsequent wide range of geographically diverse collateral damage that can result from the release of malware. Moreover, while this approach would certainly not solve the threat of correlated risks, it might reframe the risk correlation challenges that insurers face in modeling and covering cyber risks. By allowing the disentangling of different victims affected by the same piece of malware, or other attack vector, insurers might be able to reconsider how they can use the different threats that their policyholders face to allow for more diversification of their risk pools. For instance, this might allow for the risks that critical infrastructure operators face to be treated differently from those faced by other firms—even if all of those policyholders could be affected by the same piece of malicious code. It will still be the case that a single piece of malware can cause widespread and varied damages to many victims across different sectors and locations, but perhaps for insurance purposes, it would make more sense to consider which of those types of damages are

covered or not, rather than arguing over which types of attacks are or are not excluded from a policy.

Over time, war exclusions in insurance policies have been shaped by a series of historical events to encompass an increasingly broad range of activities carried out by a variety of different actors. As concerns that these exclusions may be overly broad (when it comes to cyberattacks) force insurers to start crafting explicit inclusions for cyberterrorism activity, it may be time to consider whether the historical emphasis of these exclusions on being able to definitively identify the perpetrator and motive of such attacks is ill-suited to the nature and breadth of cyberattacks. Instead, there may be more value in predicating such exclusions of large-scale cyberattacks that present the possibility of significantly correlated risks on their particular victims, impacts, and scale—characteristics that are both more easily verified and allow for more granular distinctions in the cyber domain.

INSURING EVOLVING TECHNOLOGY

ASAF LUBIN*

ABSTRACT

The study of the interaction between law and technology is more critical today than ever before. Advancements in artificial intelligence, information communications, biological and chemical engineering, and space-faring technologies, to name but a few examples, are forcing us to reexamine our traditional understanding of basic concepts in torts and insurance law.

Yet, few insurance professionals and scholars will identify themselves as working in the field of "law-and-technology." For many of them, technology is "just a fact about the world like any other," as Ryan Calo once put it, not one that always merits "special care."[1]

This short paper is an attempt to build a first-of-its-kind bridge between these two scholarly silos. Directed at an insurance audience, the paper attempts to draw attention to a body of law-and-technology scholarship that has so far gone mostly unnoticed by insurance professionals.

The paper is built on the premise that insurance lawyers, whose business model depends on the mitigation of losses from technological harm, are not dramatically dissimilar from their law-and-technology counterparts. Both are fascinated by the same set of questions: if, when, and how, might

---

* Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, a Visiting Fellow at the Information Society Project of Yale Law School, a Visiting Scholar at the Federmann Cybersecurity Center at Hebrew University of Jerusalem, a Fellow at the Center for Applied Cybersecurity Research at Indiana University, and a Visiting Fellow at the Nebraska Governance and Technology Center at the University of Nebraska. I wish to thank Dan Schwarcz, Gus Hurwitz, Demet Batur, Matthew Schaefer, Tammi Etheridge, and João Marinotti for terrific feedback on earlier drafts of this paper. I further wish to thank all the participants of the "Cyber Cyber Insurance Law Conference" organized jointly by University of Connecticut Insurance Law Center and the University of Minnesota Law School, as well as participants in the Nebraska Governance and Technology Center Fellows' Workshop and the Henry Jackson Society Cyber Insurance event. Finally, I wish to thank the editors of the Connecticut Insurance Law Journal for their consideration of this piece.

[1] Ryan Calo, *Commuting to Mars: A Response to Professors Abraham and Rabin*, 105 VA. L. REV. 84, 88 (2019).

private and public regulation mitigate losses resulting from technological risk. The paper draws key concepts from the law-and-technology literature to explore the effectiveness and utility of regulation in mitigating risks from emerging, evolving, and disruptive technologies. The paper further identifies the different phases in technology's life cycle and discusses the challenges that each of these phases introduces on the insurance market.

Relying on cyber insurance as its primary case study, the paper concludes by applying these insights to an assessment of a recent state-wide regulation, the New York Cyber Insurance Risk Framework, the first of its kind in the country. The paper demonstrates the promise and pitfalls of this type of regulation, taking into account broader trends in the cyber insurance market.

TABLE OF CONTENTS

INTRODUCTION

On March 12, 2021, the University of Minnesota and the University of Connecticut Insurance Law Center co-organized *A Cyber Cyber Insurance Conference* to examine the current state of our evolving cyber

insurance markets.[2] The organizers wisely devoted one of the panels to the unique position of government in fostering these markets.[3] As the event's website further noted, panelists were called to "explore what state and federal governments can, and should, do to promote more robust cyber insurance markets."[4]

As I was contemplating my written contribution for this symposium, I was struck by just how much has been written over the years on this very topic. Academics, international organizations, and cyber insurance specialists have produced mountains of lengthy and persuasive accounts of possible areas for regulatory reform.[5] Jay Kesan and Carol Hayes, for

---

[2] For more information about the conference, see *The Role of Law and Government in Cyber Insurance Markets: A Cyber Cyber Insurance Conference*, UNIV. OF CONN. SCH. OF L.: INS. L. CTR., https://events.uconn.edu/event/78763/2021-03-12 (last visited Jan. 31, 2022).

[3] *Id.*

[4] *The Role of Law and Government in Cyber Insurance Markets: A Cyber Cyber Insurance Conference,* EVENTBRITE, https://www.eventbrite.com/e/the-role-of-law-and-government-in-cyber-insurance-markets-registration-133229401727 (last visited Jan. 31, 2022) (reservation website).

[5] *See, e.g.*, OECD, ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT 135–37 (2017) [hereinafter OECD REPORT] ("Governments could contribute to the availability of data on past cyber incidents, forward-looking analyses on the changing nature of the risk and on the effectiveness of security practices, including through the development or promotion of cyber security standards. Governments should also closely monitor the market developments and consider if there is a need to intervene to encourage greater clarity on coverage or to support the management of accumulation risk."); EUR. INS. & OCCUPATIONAL PENSIONS AUTH., UNDERSTANDING CYBER INSURANCE – A STRUCTURED DIALOGUE WITH INSURANCE COMPANIES 25 (2018) (exploring the following potential contributions of regulations: (1) regulation of appropriate pricing and monitoring of the risks, including potential aggregation risks; (2) promotion of incident reporting and exchange of information; (3) enhancing a better understanding of risks; (4) introduction of minimum IT and Information security standards; (5) increase the level of awareness and prudence of new entrants (both insurers and buyers); (6) ensure adequate capital requirements against underwriting risks; (7) prevention of contagion in case of bigger scale); Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1499–500 (2017) (proposing "a strict-liability rule for harms deriving from cyber-incidents" noting further that "this rule would impose administratively defined statutory damages, but firms that have cyber insurance policies covering third-party harms would only pay the lesser of those statutory damages or actual provable damages for insured claims."); Minhquang N. Trang, Note, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy*

example, have discussed the prospect of "government subsidies for both insurance and security technology."[6] Michael Faure and Bernold Nieuwesteeg highlighted the role that government regulation of cybersecurity practices could play in setting normative cues for cyber insurance, particularly in the context of cyber risk pools.[7] Jan Lemnitzer called on governments to: develop minimum cybersecurity standards for small-to-medium businesses ("SMEs"), set up a claims database to increase data sharing, and announce the intention to make cyber insurance compulsory for SMEs in the near future.[8] Kenneth Abraham and Daniel Schwarcz have explored the prospect of a federal reinsurance program for cyber catastrophes.[9] Daniel Woods and Andrew Simpson have gone even further by mapping out no less than twenty-three different possible government interventions, breaking them down into six general themes, which were then introduced as part of an overarching framework and research roadmap for future scholarship.[10]

Regulation to Prevent and Mitigate Data Breaches, 18 MINN. J.L. SCI. & TECH. 389 (2017) (calling for a mandatory cyber risk regime); Brendan Heath, Note, *Before the Breach: The Role of Cyber Insurance in Incentivizing Data Security*, 86 GEO. WASH. L. REV. 1115, 1137–39 (2018) (discussing governmental regulatory options around standard setting and information dissemination); Nehal Patel, Note, *Cyber And TRIA: Expanding the Definition of An "Act of Terrorism" to Include Cyber Attacks*, 19 DUKE L. & TECH. REV. 23 (2021) (proposing amendments to the Terrorism Risk Insurance Act so that the Act more clearly covers acts of cyberterrorism); Kyle D. Logue & Adam B. Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, 28 CONN. INS. L.J. (forthcoming 2021) (manuscript 1) (proposing a "limited ban on indemnity for ransomware payments with exceptions for cases involving threats to life and limb, coupled with a mandate that property/casualty insurers provide coverage for the other costs of ransomware attacks.").

[6] Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 273–76 (2017).

[7] Michael Faure & Bernold Nieuwesteeg, *The Law and Economics of Cyber Risk Pooling*, 14 N.Y.U. J.L. & BUS. 923, 959 (2018).

[8] Jan Martin Lemnitzer, *Why Cybersecurity Insurance Should be Regulated and Compulsory*, 6 J. CYBER POL'Y 118, 125–26, 128–31 (2021).

[9] Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of Cyber Insurance Catastrophe*, 27 CONN. INS. L.J. 1, 64–66 (2021).

[10] Daniel Woods & Andrew Simpson, *Policy Measures and Cyber Insurance: A Framework*, 2 J. CYBER POL'Y 209, 221 tbl.2 (2017).

Admittingly, I also contributed to this growing heap of cyber insurance regulation scholarship. In my latest work, I relied on public policy arguments to make the case for a set of governmental interventions in the markets, particularly around the indemnification of: "(1) acts of cyber terrorism or state-sponsored cyber operations; (2) extortion payments for ransomware attacks; and (3) administrative fines for violations of statutory data protection regulations."[11]

It is important to note that all of these proposals have yet to be implemented in any meaningful way, including in North America,[12] the largest cyber insurance market in the world.[13] While some changes have certainly occurred around the margins,[14] for the most part, the status quo on

---

[11] Asaf Lubin, *Public Policy and the Insurability of Cyber Risk*, 5 J.L. & TECH. TEX. (forthcoming 2022) (manuscript at 1–2).

[12] The National Defense Authorization Act for Fiscal Year 2021 includes a provision for Government Accountability Office (GAO) to study the U.S. cyber insurance market. H.R. 6395, 116th Cong. 33 (2020) (enacted). In May 2021 GAO produced a report summarizing many of these proposals and submitted them to the appropriate congressional committees and the Secretary of the Treasury for consideration. To date, it does not appear that any substantive measures have been taken to implement the report's proposals. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET (2021).

[13] *World Cyber Insurance Market to Reach $14 Billion by 2022: Report*, BUS. INS. (Dec. 7, 2016), https://www.businessinsurance.com/article/20161207/STORY/912310861/World-cyber-insurance-market-to-reach-$14-billion-by-2022-Report ("A report by U.S.-based market research firm Allied Market Research has said that the global cyber insurance market is expected to grow at a compounded annual growth rate of 28% between 2016 and 2022 to reach $14 billion by 2022 . . . . North America is expected to hold the largest cyber insurance market share during the forecast period, driven by enforcement of data protection regulations in the United States, increases in levels of liability and legislative developments.").

[14] On the issue ransomware, the U.S. Treasury Department issued an advisory at the end of 2020, which warns companies not to pay ransom to sanctioned entities. *See* U.S. DEP'T OF TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf. In September 2021 the Department issued an updated advisory that noted that the Office of Foreign Asset Control (OFAC) when evaluating possible enforcement outcomes will consider "full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor." U.S. DEP'T OF TREASURY, UPDATED ADVISORY ON

cyber insurance remains. Why have legislatures and regulators been so slow to adopt any of these proposals? Perhaps, we have been looking at cyber insurance regulation through the wrong lens.

So far, we have focused much of our collective theorizing on *sui generis* interventions, tailored and designed to the specific risks of cyberspace.[15] But cyber insurance is, after all, merely a sub-category within a broader umbrella of insurance products, which are designated to transfer risks from evolving technologies (from a products liability insurance for 3D

POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 5 (2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf. This includes the company's "self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies . . . ." *Id.* The updated advisory extends to companies involved "in facilitating ransomware payments on behalf of victims" (thereby potentially extending the advisory to insurers and other actors involved in the negotiation with the hackers on behalf of victims). *Id.* at 4. Nonetheless, it should be noted that so far only limited enforcement action has been taken by OFAC against the payment of ransom. *See* Michael T. Borgia & Dsu-Wei Yuen, *OFAC Makes Waves in Fight Against Ransomware, but Practical Effects Unclear*, DAVIES WRIGHT TREMAINE LLP (Oct. 1, 2021), https://www.dwt.com/blogs/financial-services-law-advisor/2021/10/ofac-updated-ransomware-advisory (clarifying that at the end of 2021 OFAC issued its "first-ever sanctioning of a cryptocurrency exchange for transacting with ransomware gangs" but suggesting that "standing alone", such limited OFAC action, while "significant" by themselves, nonetheless generate "unclear" actual effects on deterrence.).

On the issue of developing cybersecurity standards, it should be noted that a few states (namely, Utah, Indiana, and Ohio) have either adopted or are in the process of adopting cybersecurity safe harbor rules. These rules provide covered entities with immunity from liability in state courts for any cybersecurity or data breach, subject that the company commits and complies with certain cybersecurity standards and frameworks laid down in the law. *See generally New Ohio Law Creates Safe Harbor for Certain Breach-Related Claims*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Nov. 5, 2018), https://www.huntonprivacyblog.com/2018/11/05/new-ohio-law-creates-safe-harbor-certain-breach-related-claims/; Romaine Marshall, *Utah Considers a Cybersecurity Safe Harbor as Ransomware Runs Rio*t, JD SUPRA: GLOB. PRIV. & SEC. BLOG (Feb. 26, 2020), https://www.jdsupra.com/legalnews/utah-considers-a-cybersecurity-safe-96201/; Gretchen M. Rutz, John L. Landolfi, Christopher L. Ingram, Christopher A. LaRocco & Sarah Spector Boudouris, *Indiana Attorney General to Create Safe Harbor for Businesses that Implement Reasonable Cybersecurity Plans*, LEXOLOGY (Sept. 28, 2020), https://www.lexology.com/library/detail.aspx?g=da29facf-7ea3-4439-ba25-28b5479577b6.

[15] *See, e.g.*, Jeffrey L. Vagle, *Cybersecurity and Moral Hazard,* 23 STAN. TECH. L. REV. 71, 85 (2020) (discussing the "*sui generis* principal-agent problem" of cybersecurity).

printed products[16] to automobile insurance for autonomous vehicles[17]). Might we, therefore, be better served, when thinking about the utility of regulating these markets, if we considered the larger network effects at the intersection of torts, insurance law, technological evolution, and social adoption?

It is undisputed that "evolving technologies generate novel questions and that these questions sometimes give rise to thorny cases."[18] What is more fraught, however, is the idea, taken up by law-and-technology scholars, that questions motivated by different technological changes and dynamics nonetheless share some underlying similarities.[19] For the law-and-technology folk, these questions arise for similar reasons and are answered in similar ways, justifying the adoption of a single unified theory.[20] As Lyria Moses argued: "[r]ecognizing the similarities between problems arising in different technological contexts creates the possibility of learning from the consequences of past legal responses to technological change."[21]

Unfortunately, legal analysis is the land of doctrinal segregation and isolationism. "Lawyers tend to break along technological lines (health lawyers, cyber-lawyers, etc.) or doctrinal lines (contract lawyers, tort lawyers, etc.)."[22] While legal specialization is certainly welcome—especially where it aims to improve the quality of legal service and reasoning while reducing the costs of conducting research and analysis[23]—at times it is hindering and even blinding. After all, insurance lawyers whose business model depends on the mitigation of losses from technological harm are not

---

[16] *See, e.g.*, Jordan Lipp & Steven Michalek, *3D Printing: Product Liability, Professional Liability and Other Tort Aspects of the Burgeoning Industry*, DEF. COUNS. J., Apr. 2020, at 1, 6 (2020); TRAVELERS INDEM. CO., HAVE YOUR 3D PRINTED CAKE AND EAT IT TOO 17 (2016), https://www.travelers.com/iw-documents/business-insurance/tech-3D-whitepaper-BTCWH.0003-D.pdf.

[17] Automated and Electric Vehicles Act, 2018, c. 18 (U.K.), https://www.legislation.gov.uk/ukpga/2018/18/contents (the act applies the existing insurance infrastructure and requirements from traditional automobiles to autonomous vehicles).

[18] Mason v. Mach. Zone, Inc., 140 F. Supp. 3d 457, 469 (D. Md. 2015).

[19] *See* Lyria Bennett Moses, *Why Have a Theory of Law and Technological Change?*, 8 MINN. J.L. SCI. & TECH. 589, 594 (2007).

[20] *See id.*

[21] *Id.* at 598.

[22] *Id.* at 594.

[23] *See generally* Clarke B. Rice, Comment, *Legal Specialization: A Proposal for More Accessible and Higher Quality Legal Services*, 40 MONT. L. REV. 287, 288 (1979).

dramatically dissimilar from their law-and-technology counterparts. Both are fascinated by the same set of questions: if, when, and how, might private and public regulation mitigate losses resulting from technological risk?

This short paper is an attempt to build a first-of-its-kind bridge between these two scholarly silos.[24] Directed at an insurance audience, the paper attempts to draw attention to a body of law-and-technology scholarship that has so far gone mostly unnoticed by insurance professionals. The paper is divided into three parts. Part I identifies the different phases in a technology's life cycle and discusses the challenges that each of these phases introduces on the insurance market for risks resulting from technology's continuous evolution. Part II then moves to explore the law-and-technology literature to distill key understandings about the effectiveness and utility of governmental interventions in mitigating risks from emerging, evolving, and disruptive technologies. This section identifies three primary lessons learned, focusing on the intersections between technology and classification, regulation, and globalization. Finally, Part III returns to the cyber insurance debate to apply these lessons. In particular, the section looks to assess the merits of the New York Insurance Regulator's recent Cyber Insurance Risk Framework[25] as the first ever state-wide cyber insurance regulation in the United States. The paper discusses the promise and limits of this regulation in the broader context of the insights from law-and-technology literature and emerging trends in the cyber insurance market.

---

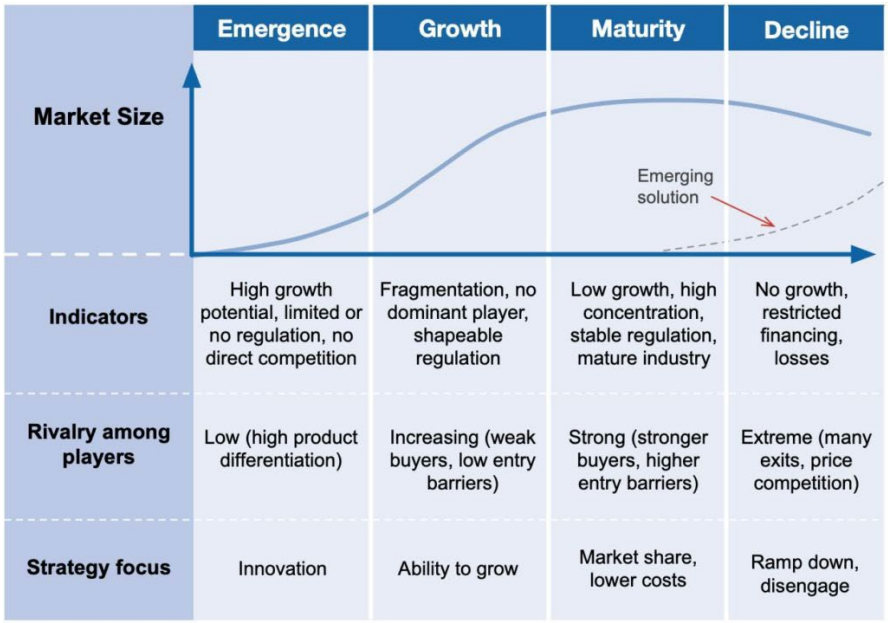
[24] Ryan Calo, responding to a paper by Kenneth Abraham and Robert Rabin on liability and insurance for autonomous vehicles, demonstrated the existence of these scholarly silos. He noted, "[t]he puzzle of how to deal with the contingency of technology and its social impacts is not limited to driverless cars, but endemic to law and technology scholarship. Personally, I doubt Professors Abraham and Rabin—each renowned scholars of civil liability—identify themselves as working in 'law and technology' as such. I imagine that for the authors, the ascendance of automated vehicles is just a fact about the world like any other, as the progress of technology often is. In my experience, however, reasoning about technological change sometimes requires special care." Calo, *supra* note 1, at 87–88 (2019) (footnote omitted).

[25] Letter from Linda A. Lacewell, Superintendent, N.Y. State: Dep't Fin. Servs., to All Authorized Prop./Cas. Insurers (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

I. BETWEEN TORTS, INSURANCE, AND TECHNOLOGICAL EVOLUTION

Technological changes are those involving "any tool or technique, any product or process, any physical equipment or method of doing or making, by which human capability is extended."[26] Such extensions can take myriad forms. The invention of the first iPhone is different from the invention of the iPhone 8. While both are technological changes extending human capability, one is emerging and disruptive, while the other offers a minor expansion within an already established line of innovation, causing far limited ripple effects.[27]

Illustration 1: Phases of an Industry Life Cycle[28]



---

[26] DONALD A. SCHON, TECHNOLOGY AND CHANGE 1 (Dell Publ'g Co. 1967)

[27] *See* Peter Huber, *Safety and the Second Best: The Hazards of Public Risk Management in the Courts*, 85 COLUM. L. REV. 277, 298 (1985) ("New products and processes, though never risk-free in themselves, usually prove to be less hazardous than the older, manmade substitutes they replace.").

[28] SUN WU, STRATEGY FOR EXECUTIVES 21 (Strategy for Execs. ed., 2019 ed. 2019).

As technology matures, our understanding of the risks associated with its deployment and use changes.[29] This includes both first-party harms (those harms that first adopters of the technology might incur directly from using such an emerging technology) and third-party harms (the possible liabilities for damages to others from the development and deployment of a new technology).[30] The latter harms are perhaps even more fundamental as the introduction of such liability could significantly stifle creativity and innovation.[31] In thinking about technological risk, its evolution over time, and its interplay with insurance as a mitigating tool, we may wish to rely on a classic industry life-cycle model. At each stage of the model—from the embryotic pre-emergence stage, to the emergence stage, to the growth stage, to the maturity and ultimate decline stages—different kinds of insured risks could be potentially introduced, and those may impact different categories of policyholders along the supply chain in different ways: from developers, to manufacturers, to distributors, to consumers.

Especially at the embryotic and emergent phases, where technology is most unstable, challenges would arise in both torts and insurance around the issue of liability.[32] Indeed, the law often treats developers and first

---

[29] *See The Evolution of Risk in the Face of Technology,* ZURICH (Nov. 10, 2014), https://www.zurich.com/en/knowledge/topics/global-risks/the-evolution-of-risk-in-the-face-of-technology (discussing how evolving technology generates "fresh risks.").

[30] As applied in the context of cyber insurance specifically see Lubin, *supra* note 11, at 6–7.

[31] *See, e.g.*, Fred Roeder, *How Liability Lawsuits Drive Up Drug Prices, Stifle Innovation, and Harm Patients*, CONSUMER CHOICE CTR. (May 7, 2020), https://consumerchoicecenter.org/how-liability-lawsuits-drive-up-drug-prices-stifle-innovation-and-harm-patients/; U.S. CHAMBER INST. FOR LEGAL REFORM, THE FUTURE OF AI LIABILITY IN THE EU: PROTECTING CONSUMERS WITHOUT STIFLING INNOVATION 20 (2020) (discussing how changes to the existing liability regime in AI regulation could stifle innovation).

[32] *See* Dennis R. Connolly, *Insurance: The Liability Messenger, in* PRODUCT LIABILITY AND INNOVATION: MANAGING RISK IN AN UNCERTAIN ENVIRONMENT 131, 135 (Janet R. Hunziker & Trevor O. Jones eds., 1994) ("[T]he more scientifically advanced the product, the more uncertainty it is likely to engender in insurers. Precisely because it is such a departure from other products, it has no track record and thus provides no solid basis for predicting and pricing the risks involved."); Peter W. Huber, *Junk Science in the Courtroom: The Impact on Innovation, in* PRODUCT LIABILITY AND INNOVATION: MANAGING RISK IN AN UNCERTAIN ENVIRONMENT 138, 138 (Janet R. Hunziker & Trevor O. Jones eds., 1994) ("It is the new venture with the unfamiliar product that can least tolerate the

adopters "as taking their chances with a technology," [33] assigning all costs for potential harms from creating and using the technology to them.[34] Courts "greatly prefer natural, old, or established hazards to those deriving from new technologies."[35] As such, their early rulings may set chilling effects on continued development and use of the technology.[36] Insurers, in turn, will either not offer the coverage or offer only limited protections with significantly high premiums.[37]

Government interventions at this stage could focus on creating a counterbalance to these inherent disincentives within the law on innovation, research, and design of new technologies. This is because "[t]here is hardly a product in use today—a car, plane, boiler, municipal water system, drug, vaccine, or hypodermic syringe—that is not many times safer than its counterpart of a generation or even a decade ago."[38] So, to the extent that "[i]nnovation and technological change . . . reduce risk,"[39] the government would benefit from summoning the courage and implementing the incentive structure so that developers and users may survive the turbulent embryotic and emergent period.[40]

---

extra measure of instability from the legal environment that does not provide predictable results.").

[33] Kyle Graham, *Of Frightened Horses and Autonomous Vehicles: Tort Law and Its Assimilation of Innovations*, 52 SANTA CLARA L. REV. 1241, 1260 (2012).

[34] *See* Connolly, *supra* note 32, at 134 (noting the various ways state laws can be "insurer-unfriendly").

[35] Huber, *supra* note 27, at 307.

[36] Graham, *supra* note 33, at 1268–70.

[37] Trevor O. Jones & Janet R. Hunziker, *Overview and Perspectives, in* PRODUCT LIABILITY AND INNOVATION: MANAGING RISK IN AN UNCERTAIN ENVIRONMENT 1, 2 (Janet R. Hunziker & Trevor O. Jones eds., 1994) ("Even though product safety may have been improving, companies were experiencing more product liability cases and the size of the awards was increasing. As a result, their insurance costs were going up and for some products, insurance coverage was being withdrawn altogether.").

[38] Huber, *supra* note 27, at 298.

[39] *Id.* at 298–99.

[40] For an alternative view, one that posits that technology does not evolve in a linear way towards ultimate safety, see Vagle, *supra* note 15, at 92–94 (suggesting that the "uniquely American concept of technology advancement," as adopted by Silicon Valley, is one of "innovation-over-maintenance." According to this approach, companies prefer the ability "to rapidly move from idea to prototype to product" even if that comes at the expense of their customers' security. "One of the more significant problems with this approach is the increased risk associated with a

A more nuanced view suggests that different technologies would experience different embryotic stages, with tort and innovation interacting in different ways. Some technologies will "produce 'too many' lawsuits" while others might produce "too few."[41] This is because legal uncertainty "can cut two ways."[42]

> Uncertainty as to the prospect, viability, and magnitude of tort claims regarding an invention may chill its development and diffusion. But uncertainty as to matters such as the existence of a cause of action and the likelihood of recovery also may stifle the filing of claims that attack the innovation as unreasonably dangerous.[43]

The nature of the technology, the scope and magnitude of its likely harms, and the volume of harmful occurrences that actually materialize, would all play a role in the cost-benefit analysis behind prospective litigation and liability insurance.

In any event, a common theme along the time continuum of the technology life cycle is the notion that "uncertainty does give way to knowledge over time. Society learns as it produces and assembles information about technological hazards."[44] With information comes a better ability to regulate and set expectations of behavior and duties of care; with that the risk becomes "fully assimilated within everyday tort law."[45] Insurers appreciate this level of stability, which translates in turn into lower premiums and higher caps as risk modeling and management solidifies.

But law continues to interact with the technology even after it has fully matured. Danielle Citron carefully described how law, as designed by

---

company's inability (or unwillingness) to seriously consider the negative consequences of their design decisions in the race to innovate.").

[41] *See* Graham, *supra* note 33, at 1269.

[42] *Id.* at 1268.

[43] *Id.* at 1268–69.

[44] Mary L. Lyndon, *Tort Law and Technology*, 12 YALE J. ON REG. 137, 141 (1995).

[45] Graham, *supra* note 33, at 1242. If to use Baker's terminology, once a technology reaches a certain maturity then "tort doctrine and the consistent behavior of insurance adjusters" will begin to converge. Tom Baker, *Liability Insurance as Tort Regulation: Six Ways That Liability Insurance Shapes Tort Law in Action*, 12 CONN. INS. L.J. 1, 12 (2005). This is because "street level bureaucrats" will over time begin to take over "the bulk of the tort law universe" to a point where tort law and insurance practice engage in regular and mutually beneficial conversation. *Id.*

courts, regulators, and legislatures, might interact with technology throughout its life cycle:

> First, it recognizes the new form of harm, but not the benefit that the new technology has occasioned. This drives the law to adapt existing theories of liability to reach that harm. Second, after the technology's benefits become apparent, the law abruptly reverses course, seeing its earlier awards of liability as threats to technological progress and granting sweeping protection to the firms in the new industry. Finally, once the technology becomes better established, the law recognizes that not all liability awards threaten its survival. It then separates activities that are indispensable to the pursuit of the new industry from behavior that causes unnecessary harm to third parties.[46]

External actors, such as reinsurers, might need to step in at different stages to offer an intervention. Think about developments in engineering technologies in the United States in the nineteenth and early twentieth centuries. "[T]he scope of challenging engineering projects—from larger and more complex manufacturing, infrastructure, and aircraft—were now beyond the capacity and expertise of a single insurer. These risks required a new level of expertise and risk management not readily available within the ranks of US insurers."[47] Established European reinsurers, such as Swiss Re, "extended their capacity to reinsure these single, large risks in collaboration with insurers and large corporate clients."[48] Reinsurance thus stepped in to provide a safety net and a necessary degree of assurance for innovation to be tested, proven, and ultimately assimilated.

Where insurance and reinsurance are not available, the government might take a more active role. Consider the United States government indemnification frameworks for commercial space-flight operators. The operators are required to obtain "third-party liability insurance in the amount of the maximum probable loss (MPL), according to a calculation performed

---

[46] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 115 (2009) (footnotes omitted).

[47] SWISS RE CORP. HIST., A HISTORY OF US INSURANCE 24 (2017), https://www.swissre.com/dam/jcr:36ebe594-097d-4d4d-b3a7-2cbb8d856e85/150Y_Markt_Broschuere_USA_EN_Inhalt.pdf.

[48] *Id.*

by the FAA [Federal Aviation Administration]."[49] Where the third-party liability claims exceed the MPL, "the government has in essence made a statutory promise to pay for the next tier, or tranche, of up to $2.8 billion dollars in any third-party liability claims faced by the space-flight entity."[50] Because the advancement of a vibrant commercial space industry is a matter of national security importance to the United States and its economy, the government is willing to step in and offer this promise.[51]

II. LESSONS LEARNED FROM LAW AND TECHNOLOGY LITERATURE

A complex set of questions goes into an *entity's decision to generate new law* in a technologically evolving environment. These questions include: What do we mean by "*new law"*? Who is the "*entity*" that makes that decision? And what forms might "*law generation*" take? Law-and-technology scholars have been fascinated by these questions. Their ability to answer these questions effectively is rooted in their willingness to approach such questions not solely from a legal or economic perspective. Rather, many of these scholars adopt an interdisciplinary lens that is socio-legal. For them, regulation is not merely the "promulgation of an authoritative set of rules, accompanied by mechanisms . . . for monitoring and promoting compliance with these rules."[52] They step outside of what Christel Koop and Martin Lodge call the "prototype regulation," the public interventions that are "intentional and direct."[53] Instead, they adopt a far higher level of abstraction, seeing regulation as a varied set of "mechanisms of social control."[54]

---

[49] Matthew Schaefer, *The Need for Federal Preemption and International Negotiations Regarding Liability Caps and Waivers of Liability in the U.S. Commercial Space Industry*, 33 BERKELEY J. INT'L. L. 223, 230 (2015).

[50] *Id.* at 231.

[51] *Id.* at 233–34. Note that the government may intervene in other ways. The government can promote international standards on liability through diplomacy. *Id.* at 242–44. The government can also legislate immunity from liability under certain circumstances. *See, e.g.*, *id.* at 254 tbl.1 (discussing legislation on immunity for space activities in Virginia, Colorado, Texas, New Mexico, California, and Florida).

[52] A READER ON REGULATION 3 (Robert Baldwin, Colin Scott, & Christopher Hood eds., 1998).

[53] Christel Koop & Martin Lodge, *What is Regulation? An Interdisciplinary Concept Analysis*, 11 REG. & GOVERNANCE 95, 105 (2017).

[54] A READER ON REGULATION, *supra* note 52, at 4.

The section below offers a non-exhaustive summary of four of the key insights that scholars in this area have promulgated around technological regulation. It includes the intersection between technology and classification, technology and the regulator, and technology and globalization. When we think about insurance regulation, specifically the regulation of insurance for evolving technologies, we might benefit from exploring these insights.

A. TECHNOLOGY AND CLASSIFICATION

New technologies "may take earlier regulations by surprise."[55] These technologies introduce new risks and reduce old ones; they trigger new activities, and thereby fall into "regulatory lacunae" or "present regulatory misfits."[56] Underlying all of these is the sense that "emerging technologies challenge existing regulatory paradigms."[57] Indeed, both judge-made common law and statutory regulation depend on categorizations that evolve over time. In this regard, rule-appliers might be tempted to fit square pegs into round holes. Law-and-technology scholars highlight the fact that any such legal categorization is a mere "construct" where "the dispute and context are the immutable reality."[58] As such, "[i]f legal categories do not fit a new reality well, then it is the legal categories that must be re-evaluated."[59]

Insurance law has its own set of traditional classifications. Insurers often rely on "classification criteria" in the "marketing, underwriting, and pricing" stage.[60] These are a set of "factors insurance companies use to assign individual applicants to groups differing in riskiness for the purpose

---

[55] Anupam Chander, *Future-Proofing Law*, 51 U.C. DAVIS L. REV. 1, 15 (2017).

[56] *Id.*

[57] *Id.* at 16. *See also* Gregory N. Mandel, *Legal Evolution in Response to Technological Change*, *in* LAW, REGULATION, AND TECHNOLOGY 225, 227 (Roger Brownsword, Eloise Scotford, & Karen Yeung eds., 2017) (noting three lessons that are "generalizable cross a wide variety of technologies, legal fields, and contexts. These three lessons are: (1) pre-existing legal categories may no longer apply to new law and technology disputes; (2) legal decision makers should be mindful to avoid letting the marvels of new technology distort their legal analysis; and (3) the type of legal disputes that will arise from new technology are often unforeseeable." (citation omitted)).

[58] Mandel, *supra* note 57, at 234.

[59] *Id.*

[60] Regina Austin, *The Insurance Classification Controversy*, 131 U. PENN. L. REV. 517, 517 (1983).

of determining whether insurance will be sold to them, and, if so, at what cost and on what terms."[61]

New technological risks might result in breaking away from paradigmatic insurance classifications. Take for example the size of a company. Oftentimes, size is a useful category for determining the nature and scope of a risk posed by a prospective client. But in the cyber insurance domain, small companies could pose significant risk for cyber incidents (e.g., a business model that centers around the collection and transfer of large volumes of personally identifiable information),[62] whereas a large company might pose a minimum risk.[63]

When addressing new technological risks, insurers frequently use technology as well. The use of insurtech and lawtech tools open the door for predictive analysis and the ability to mine vast data troves to provide insights into the actuarial process.[64] Insurers and reinsurers alike "can better clean and process their data and identify indicators for known and unknown

---

[61] *Id.*

[62] *See* Eric Chabrow, *Cyber-Insurance: One Size Doesn't Fit All*, SEC. AGENDA, Mar. 2013, at 14, 15, https://fa94d5c47256403c613d-7164cafcaac68bfd3318486ab257f999.ssl.cf1.rackcdn.com//security-agenda-re-assessing-risk-evolving-threats-require-new-approach-to-risk-management-pdf-h-41.pdf (Citing Kevin Kalinich, global network and cyber-risk practice leader for Aon Risk Solutions, an insurance brokerage, who said that "[t]o the extent that an entity has a large number of personally identifiable information records, then there's a much bigger chance of exposure.").

[63] *Cf.* OECD REPORT, *supra* note 5, at 74 ("Insurance companies also focus significant attention on the company's security practices and policies, depending on company size and amount of coverage being sought. For smaller companies/coverage amounts, the underwriting process will focus on basic cyber security practices such as use of a firewall, anti-virus/malware software and data encryption, as well as frequency of data backups and use of intrusion detection tools.")

[64] *See* Agnieszka McPeak, *Disruptive Technology and the Ethical Lawyer*, 50 U. TOL. L. REV. 457, 461–68 (2019) (discussing lawtech). *See, e.g.*, Gina Clarke, *How Your Insurance Quote Is Powered by Artificial Intelligence*, FORBES (Jan. 21, 2019, 6:50 AM), https://www.forbes.com/sites/ginaclarke/2019/01/21/how-your-insurance-quote-is-powered-by-artificial-intelligence; *How Strong Is the Impact of Artificial Intelligence in the Insurance Industry?*, MEDIUM: INMEDIATE.IO (Aug. 1, 2019), https://inmediatesg.medium.com/how-strong-is-the-impact-of-artificial-intelligence-in-the-insurance-industry-34bd93ad47ac.

risks."[65] Indeed, machine learning "can recognize patterns that human underwriters never thought to investigate, or those that correlate with risk so subtly that they were not previously identified."[66] Insurers may also integrate technology throughout their business by encouraging clients to wear connected devices and place advanced sensors in their vehicles or on their networks.[67] Such "trove of personal data and corresponding analytics" may be used to "limit major risks before they occur,"[68] personalize insurance offerings,[69] engage in continuous underwriting,[70] and detect insurance fraud more easily.[71]

At the same time, however, "[t]he iterative, unsupervised analysis used by AI to price insurance policies may undermine the limited state and federal protections that exist to protect vulnerable groups and suspect classes from higher prices."[72] This adds to a growing list of potential inequalities that could emerge from an overutilization of technology for insurance marketing purposes, including: algorithmic bias, data harvesting, privacy intrusions, insurance data breaches, and ultimately discrimination.[73] Anya Prince and Daniel Schwarcz have, for example, demonstrated how the use of

---

[65] Jennifer Coleman, *Risk Management Implications and Applications of Artificial Intelligence Within the (Re)Insurance industry*, *in* THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE (RE)INSURANCE SECTOR 19 (SCOR SE ed., 2018), https://www.scor.com/en/download/file/25130?token=def50200e8f41bdba1037e4db3993f17964956470fd96275cfcbc2b7217828b4cba870aa6bc069b54009f44ccf32ee1e13328782e368382e06b2b64cc7fdeb1a566931b95cbcd7177e5dbbf09fc5d7bd8d8860761dbe1e7eb83a4eddf4017ce3ef74840f1e3f67e4dc1cd03727ef1d146f3474a76fa310f66b755c9589b2e40f8ed80ddea9.

[66] Samuel Lewis, *Insurtech: An Industry Ripe for Disruption*, 1 GEO. L. TECH. REV. 491, 494 (2017).

[67] *Id.* at 494–95. *See also* Yehonatan Shiman, *Expected Bad Moral Luck*, 25 CONN. INS. L.J. 112, 149 (2018) (noting that insurtech based "underwriting procedures rely on information gathered through mass-data collections from smart-phones, web searches, wearable sensors, and meta-data, among others to make better-informed decisions about an applicant's risk level. Access to this information's quantity and quality better positions insurance companies to assess risk, set representations and warranties, as well as mitigate exposure to moral hazard and fraud." (footnotes omitted)).

[68] Lewis, *supra* note 66, at 494.

[69] *Id.* at 495–96.

[70] *Id.* at 496–97.

[71] *Id.* at 497.

[72] Rick Swedloff, *The New Regulatory Imperative for Insurance*, 61 B.C. L. REV. 2031, 2058 (2020).

[73] *See generally id.* at 2057–70.

AI by insurance would inevitably result in "proxy discrimination" which could prove an "increasingly fundamental challenge to anti-discrimination regimes."[74] In other words, the use of these technologies by insurance agencies could by itself introduce new regulatory challenges and complicate existing legal classifications.

B. TECHNOLOGY AND THE REGULATOR

Rebecca Crootof and B.J. Ard introduce a methodological framework for rule-appliers and rule-prescribers in structuring their responses to what they call "TechLaw" questions.[75] The framework may be summarized in the following three-pronged analysis.

First, the assessor is called to "[i]dentify the type(s) of legal uncertainty at issue with regard to an artifact [new technology], [tech-enabled] actor, or activity [tech-enabled conduct]."[76] In this phase, the assessor will explore three questions: (a) "[w]hether and how existing law applies" (and what legal gaps and overlaps might have been erected); (b) "[w]hether existing law accomplishes its intended aims" (and in what ways might it be under or over inclusive); and (c) "[w]hether existing legal institutions have the authority, competence, or legitimacy to resolve applications and normative uncertainties."[77]

Second, the assessor is asked to "[e]valuate [the technology's] potential benefits and risks" and "consider who is likely to be impacted and their ability to mobilize for change."[78] Based on this information, the assessor might adopt a permissive approach (a "[p]resumption favoring less regulation" where the "tech's opponents bear [the] burden of changing law") or a precautionary approach (a "[p]resumption favoring preemptive regulation" where the "tech's proponents bear [the] burden of changing law).[79]

At the final stage, the assessor "determine[s] which response(s) will best resolve the [tech-fostered] legal uncertainty."[80] The assessor may

---

[74] Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1264 (2020).

[75] Rebecca Crootof & BJ Ard, *Structuring TechLaw*, 34 HARV. J.L. & TECH. 347, 350 fig.1 (2021) (providing an illustration of their methodological framework).

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *Id.*

choose to "[e]xtend [e]xtant [l]aw," "[c]reate [n]ew [l]aw," or "[r]eassess the [r]egime."[81]

This analytical roadmap is extremely useful, even from the perspective of a regulator looking to regulate a new insurance market for technological risk. It provides a useful canvas and set of factors that each assessor may look at to evaluate at different junctures throughout the life cycle of the technology and as disputes arise. Nonetheless, the framework stops short of providing immediate answers to three follow-up questions: who, when, and what.

1. Who?

Who should be the assessor? Local, state, or federal legislatures and courts? State insurance regulators and attorney generals, or federal administrative and enforcement agencies? Or what about international organizations and foreign governments? What is clear to me is that the regulation of technological risk and the insurance markets associated with it requires a reconceptualization of the old McCarran–Ferguson dichotomy. The 1945 Act, passed by the 79th Congress, sought to exempt the business of insurance from most federal regulation.[82] But to think of insurance regulation in such a narrow way is unpersuasive.

The assessor or regulator can be different entities, at different times, depending on the situation. Whoever is the assessor must be mindful of their institutional capacities and pitfalls. They should be cautiously aware of the limits of their authority and the long-term consequences that a poorly made decision could have on the continued evolution of the market.

Consider, for example, the management of insurance policy language. Legislatures and regulators are far superior to courts in this area.

> The legislative and regulatory processes allow prospective implementation of changes to policy language and prospective calculation of premiums based on risks assumed by the insurer. Modifications to agreements through the judicial process, however, are primarily retrospective, long

[81] *Id.*

[82] McCarran–Ferguson Act, 15 U.S.C. §§ 1011–1015 (1945).

> after the contracts were entered into and premiums calculated and paid based on agreed-to policy language.[83]

Moreover, many insurance policies, in an attempt to future-proof their language, incorporate into their text the evolving regulation by the legislator. For example, directors and officers liability policies often include an exclusion for:

> [A]ny actual or alleged violation of any securities law, regulation or legislation, . . . any other federal securities law or legislation, or any other similar law or legislation of any state, province or other jurisdiction, or any amendment to the above laws, or any violation of any order, ruling or regulation issued pursuant to the above laws . . . .[84]

In this regard, any regulator needs to understand that by amending or extending laws, they are directly injecting themselves into the bilateral contracts between insurers and insureds, who take their cues directly from the legislation. Since "legal liability for [c]yber [r]isk is rapidly and constantly evolving,"[85] in part through state legislation and enforcement agency action, cyber insurance is particularly susceptible to this phenomenon.

But state regulation also has its limits. As Daniel Schwarcz and Steven Schwarcz have shown, "[s]tate insurance regulation is poorly equipped to address systemic risk in insurance . . . ."[86] This is due, in part, to the fact that "[d]elegating to States sole regulatory responsibilities over

---

[83] Prodigy Commc'ns Corp. v. Agric. Excess & Surplus Ins. Co., 288 S.W.3d 374, 387 (Tex. 2009) (Johnson, J., dissenting).

[84] BEAZLEY, INFORMATION SECURITY & PRIVACY INSURANCE WITH ELECTRONIC MEDIA LIABILITY COVERAGE FORM F00106SL 7 (Aug. 2011 ed., 2011), https://www.beazley.com/documents/Private%20Enterprise/Wordings/NEW%202011%20Info%20Sec%20Form%20F00106SL%20082011%20ed.pdf.

[85] Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 406 (2015)

[86] Daniel Schwarcz & Steven L. Schwarcz, *Regulating Systemic Risk in Insurance*, 81 U. CHI. L. REV. 1569, 1627 (2014). The second reason for why states tend to underperform when regulating systemic risk (beyond the "internalization principle") is the fact that state regulators "lack the necessary expertise and perspective." *Id.* at 1631. State insurance regulators are also lacking in their ability to coordinate together and with the federal government. *Id.* at 1632.

activities that produce negative externalities nationally or internationally will generally lead to underregulation of those activities."[87] Since certain cyber risks are systemic, due to common vulnerabilities and concentrated dependencies that could lead to cascading effects,[88] states cannot possibly regulate cyber insurance alone.

But it is not just states. National governments cannot be the sole insurance regulators of technological risk. Neil Doherty once wrote that the "long delays between the writing of the [insurance] contract and the realization of loss permit a substantial cumulative change in the information base" on which the policy was formulated and priced.[89] Doherty noted that "[t]hese changes arise both from legislative and judicial changes in liability rules and from judicial precedents which re-interpret insurance contract wordings."[90] As technology is not always limited by territorial line drawing, the legislative and judicial changes might occur overseas and have ripple effects at home. Examples of such international changes include: an international treaty on cyber attribution; new cybersecurity best practices from the International Standard Organization ("ISO"); changes to privacy policies promulgated by a European national data protection authority; or revised understanding of common cyber insurance clauses developed by the International Underwriting Association or Lloyd's Market Association.[91]

Moreover, the changes in the "information base" that Doherty spoke of, which impact the risk environment, can also be non-legislative and non-

---

[87] *Id.* at 1628.

[88] DAVIS HAKE, ANDREAS KUEHN, ABAGAIL LAWSON & BRUCE MCCONNELL, CYBER INSURANCE AND SYSTEMIC MARKET RISK 5 (2019), https://www.eastwest.ngo/sites/default/files/ideas-files/cyber-insurance-and-systemic-market-risk.pdf. *See also* Abraham & Schwarcz, *supra* note 9, at 11 (discussing "damage risk," "liability risk," and "coverage risk," as three prerequisites for a cyber catastrophe that could result in correlated losses for insurers).

[89] Neil A. Doherty, *The Design of Insurance Contracts When Liability Rules are Unstable*, 58 J. RISK & INS. 227, 243 (1991).

[90] *Id.* at 243–44.

[91] One example of this can be seen in the context of extraterritorial data protection legislation, such as the European General Data Protection Regulation (GDPR). *See* Commission Directive 16/679, 2016 O.J. (L 119) 1 (EU). *See also* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 142 (2020) (introducing a "Brussels Effect" as an example for utilizing European market power to force foreign corporations to comply with European data protection standards. Bradford cites to others who have described the GDPR as "unashamedly global." She notes that given both the fact that the regulation is "extraterritorial and highly inelastic" and the fact that abandoning the EU market "is not even remotely a commercially viable option" results in the EU's expansive regulatory capacity.).

judicial. They may be societal. As society discovers new technology and employs it in ways not first imagined or envisioned by its creators, the technology takes on a life of its own. What it means to be safe or negligent, efficient or inefficient, tortious or innocent, will evolve over time. They will be shaped by social customs and intuitions formed around the technology.[92] This may be a slow and incremental process, or, depending on the technology, could also rapidly move alongside technology's deployment and adoption. If private law and private ordering "draw from and reinforce social norms,"[93] as Merill has suggested, then a broader set of actors could be seen as potential norm-developers, and therefore possible regulators of this liability and insurance environment. From design decisions made by technology companies to influencers on TikTok, our collective understating of custom around new technologies will be shaped by an ecosystem larger than one state insurance regulator.

2. When?

A complex set of questions goes into deciding when to introduce a new law into a technologically evolving environment.[94] Sometimes, simply letting the market run its course can prove to be the more efficient route. Consider this historical example:

> In ancient China mandarins who ran espionage operations devised what they believed was a foolproof secret

---

[92] João Marinotti notes that even in the context of emerging and disruptive technologies, shared "social customs and intuitions can stem from cognitive effects of human perception, as well as from learned associations, whether economic, social, or otherwise." João Marinotti, *Tangibility as Technology*, 37 GA. STATE U. L. REV. 671, 709 (2021) (footnotes omitted).

[93] Thomas W. Merrill, *Private and Public Law*, *in* THE OXFORD HANDBOOK OF THE NEW PRIVATE LAW 575, 578 (Andrew S. Gold, John C.P. Goldberg, Daniel B. Kelly, Emily Sherwin & Henry E. Smith eds., 2021). *See also* Nathan B. Oman, *Private Law and Local Custom*, *in* THE OXFORD HANDBOOK OF THE NEW PRIVATE LAW 159, 172–74 (Andrew S. Gold, John C.P. Goldberg, Daniel B. Kelly, Emily Sherwin & Henry E. Smith eds., 2021) (referring to the "prevailing beliefs and practices of the community" as a source for of private law rules, further noting that courts "fit the law to the character of their particular community, with an eye to its institutions and historical development.").

[94] Colin B. Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 CARDOZO L. REV. 149, 203–05 (2001) (outlining questions for policymakers crafting international regulations for new technologies).

> communication system for spies. They shaved a spy's head, wrote a secret message on the bald skull, then waited until the spy's hair grew back, at which point he would be sent on his way. At his destination his head would be shaved again, revealing the message.[95]

If we were rule-prescribers living at that time and were worried about espionage, we might rush into setting some rules of the road for the emerging practice of "skull messaging."

Instead, we could also wait. As Jonathan Zittrain observed, "[t]he procrastination principle rests on the assumption that most problems . . . can be solved later or by others."[96] Indeed, in our historical example, the obvious was soon realized—that the months of delay required before a new set of hair grew, made the communication itself quite futile.[97]

It was this deficiency in the system that made the Greeks in 480 BCE devise the scytale as an alternative.[98] The scytale "involved writing on the length of a sheet of papyrus wound around a staff, which, when removed and sent on, was intelligible only to a recipient who had a twin staff of precisely the same diameter and length."[99] Of course, the scytale was only useful for short messages. The need to write longer secret communications is what eventually led to the discovery of invisible ink.[100]

Round and round we go as needs trigger innovation and user feedback triggers new needs, which in turn trigger new innovations. Rule-prescribers must choose wisely the right moment for a regulatory intervention in this otherwise closed loop. At the same time, they might benefit from not waiting too long. Early interventions could provide "a more

---

[95] ERNEST VOLKMAN, THE HISTORY OF ESPIONAGE: THE CLANDESTINE WORLD OF SURVEILLANCE, SPYING AND INTELLIGENCE, FROM ANCIENT TIMES TO THE POST-9/11 WORLD 20 (2007).

[96] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT 31 (2008). *See also* Yoram Dinstein, *The Recent Evolution of the International Law of Armed Conflict: Confusions, Constraints, and Challenges*, 51 VAND. J. TRANSNAT'L L. 701, 710 (2018) (suggesting that in the context of the introduction of AI to the battlefield and the "awesome conundrums" that such a weapon system introduces, "answers should lie in wait until we have a much better picture of what the technology will actually look like.").

[97] VOLKMAN, *supra* note 95, at 20 ("[I]t takes time for a full head of human hair to grow back, meaning any intelligence on that skull cannot be very timely.").

[98] *Id.*

[99] *Id.*

[100] *Id.*

objective regulatory atmosphere, before parties become entrenched and adversarial. In contrast, deferring action (usually in the name of preserving discretion and gathering information), often leads to incremental decision making, which is more susceptible to interest group influence."[101]

This tension has perfectly manifested itself in the intellectual exchange between Ryan Calo, Kenneth Abraham, and Robert Rabin with regards to autonomous vehicle liability and insurance regulation. On one side stands Calo, who claims that no one holds a "crystal ball" and that the "very prospect that dramatically distinct modalities of transportation could arise from the ability of vehicles to drive themselves seems to caution against a preemptive, administratively intense solution that forbids state legislatures or courts from experimentation."[102] On the other side stand Abraham and Rabin. As autonomous vehicles "are already on the roads being tested," they posit that "[w]e cannot afford to wait and see what the future brings over a period of decades . . . ."[103] The future, they say, "is just over the horizon. The failure to do something about that is not the equivalent of keeping our policymaking powder dry."[104]

Timing is everything in life and in law. As the book of *Ecclesiastes* teaches "[t]o every [thing there is] a season, and a time to every purpose . . . ."[105] Therefore, different kinds of regulations by different kinds of regulators will be appropriate at different times. It is therefore possible that Calo, Abraham, and Rabin are all correct in thinking that some regulations may be good for now, while others might be good for later.

3. What?

In the age of technological innovation, rulemaking can take different forms. "Many agencies regularly employ a mix of policymaking tools on a given issue—sometimes promulgating or amending a rule, sometimes bringing an enforcement action, and sometimes issuing a guidance document."[106] To increase opportunities for trial-and-error, innovation, and flexibility, regulations can be further experimented with. One type of forum

---

[101] Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175, 204 (2014).

[102] Calo, *supra* note 1, at 87.

[103] Kenneth S. Abraham & Robert L. Rabin, *The Future is Almost Here: Inaction is Actually Mistaken Action*, 105 VA. L. REV. ONLINE 91, 92 (2019).

[104] *Id.*

[105] *Ecclesiastes* 3:1 (King James).

[106] M. Elizabeth Magill, *Agency Choice of Policymaking Form*, 71 U. CHI. L. REV. 1383, 1410 (2004).

for this kind of legal incubation is the "regulatory sandboxes"– environments in which regulation can be pre-tested in a relative vacuum with real stakeholders.[107] In such a scenario, co-regulation becomes possible as collaboration is fostered between the regulator and the regulated entity.[108] In the context of cyber insurance, Israel is now attempting to become a national sandbox, a beta site for experimentation in cyber insurance regulation.[109]

Regulation does not only mean formal prescriptive top-to-bottom ordinances. Formal legal rules are but one of four types of constraints that "regulate" in the broader sense. Lawrence Lessig identified the three other constraints as, "social norms, the market, and architecture."[110] I have already elaborated on the importance of social customs and intuitions in private law and private ordering,[111] so I will briefly address the two remaining constraints.

Price points, supply-and-demand, and barriers to accessibility will impact behavior. Combined with other soft law instruments, such as "private standards, codes of conduct, certification programs, principles, guidelines, and voluntary programs,"[112] these form market constraints on the technology, which in turn shape our expectations around its functions, properties, and limits.

Choices in the design and architecture of a technology will also impact our collective understanding of its features and capacities. As noted by Paul Ohm and Blake Reid, "[w]e used to regulate things, and now we regulate code."[113] João Marinotti has shown, for example, how the

---

[107] Hilary J. Allen, *Regulatory Sandboxes*, 87 GEO. WASH. L. REV. 579, 579 (2019).

[108] For further reading on regulatory sandboxes see *id.*; Radostina Parenti, *Regulatory Sandboxes and Innovation Hubs for FinTech Impact on Innovation, Financial Stability and Supervisory Convergence, Study for the Committee on Economic and Monetary Affairs*, POL'Y DEP'T. ECON. SCI. & QUALITY LIFE POL'Y, PE 652.752, 33–38 (Sept. 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf.

[109] *See* Asaf Lubin, *Cyber Insurance as Cyber Diplomacy*, *in* CYBER WAR & CYBER PEACE IN THE MIDDLE EAST: DIGITAL CONFLICT IN THE CRADLE OF CIVILIZATION 22, 27–30 (Michael Sexton & Eliza Campbell eds., 2020).

[110] LAWRENCE LESSIG, CODE: VERSION 2.0 123 (2006).

[111] *See supra* notes 92–93 and accompanying text.

[112] Gary E. Marchant, *Governance of Emerging Technologies as a Wicked Problem*, 73 VAND. L. REV. 1861, 1866 (2020).

[113] Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1702 (2016).

"cryptographic imperatives"[114] of exclusion and control, which are embedded in the core of Bitcoin, resulted in the "establishment of a shared social custom and intuition about how bitcoins are used and what non-owners may or may not do."[115] In other words, the architecture of the technology helps regulate the legal interests and liabilities that emerge from and in response to a volatile technological space.

All of these demonstrate that when we wish to engage in the regulation of an evolving technology, say around its liability and insurance, we must adopt a broader lens. There can be different regulated entities. For example, we may think about the regulation of insurers, or of the insured; we may regulate tech providers, or their clients; we may limit our regulation to public entities, or extend it to private entities; we may focus on large corporations or particular sectors; or we may adopt a whole-market approach, including small-to-medium enterprises.

Applying these concepts in the cyber insurance context, we may be able to develop a non-exhaustive list of potential examples of both direct and indirect regulations that may be employed by different kinds of regulators at different times. What distinguishes these two categories is that whereas direct regulations target the commercial insurers themselves, indirect regulations target the legal and policy environment in which these insurers operate.

Illustration 2: Examples of Different Initiatives for Direct and Indirect Cyber Insurance Regulation

Direct Regulation	**Indirect Regulation**
Cyber Claims Information-Sharing Requirements	Data Breach Notification Laws
Security Data Depositories	State/Federal/Foreign Privacy and Data Protection Regulation
Mandatory Policy Language or Questionnaires	Subsidies for Cybersecurity Services and/or Research and Development
Governmental Insurance of Last Resort for State-Sponsored Cyber Operations and Other Acts of Cyber War or Terrorism	Cybersecurity Liability Safe Harbor Laws

[114] Marinotti, *supra* note 92, at 726.
[115] *Id.* at 728.

Direct Regulation	Indirect Regulation
Prohibition on Ransomware Payments	Liability for Tech Providers (e.g., Internet-of-Things Vendors)
Prohibition on Indemnification of Statutory Data Protection Fines	Government Exercise of its Procurement Power to Support Cybersecurity Best Practices
Standard Metrics, Requirements, and Other Data Formats for Assessment or Claims Process	National Certification of Cybersecurity Standards and Licensing of Cybersecurity Providers
Establish Insurer Liability for Providing Security Advice	International Frameworks for Cybersecurity Attribution
Make Cyber Insurance Compulsory for Certain Industries	Rules of International Law on Responsible Behavior in Cyberspace

C. TECHNOLOGY AND GLOBALIZATION

Technology, in the sense of human innovation and human progress, is a phenomenon that defies national borders. Technology has a tendency to spread and connect individuals in ways that go beyond jurisdictional lines. "A regulator sitting in Washington, D.C. considering how to approach a new technology must keep in mind that her counterpart in Brussels, Beijing, or Bogota is likely pondering the same question. She has to make decisions to regulate or not, or how to regulate, while looking over her shoulder."[116]

This lesson is particularly acute in the context of cyber insurance. This is because cybersecurity and cyber stability are matters of national and international security, and therefore are matters that are intimately connected to global political affairs. Espionage operations by a foreign nation state, like the SolarWinds hack, could have cascading effects on the markets.[117] As such, what is discussed in the United Nations Security Council in the morning may end up on the table of a commercial insurer in Connecticut by evening time. Few other insurable risks share this property. Put differently, if the Ace American Insurance Company is truly concerned with whether its wartime exclusion applies in the case of an alleged Russian ransomware

[116] Chander, *supra* note 55, at 21.

[117] For more on the SolarWinds Hack see Asaf Lubin, *SolarWinds as a Constitutive Moment: A New Agenda for the International Law of Intelligence*, JUST SEC. (Dec. 23, 2020), https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/.

attack,[118] it should focus its advocacy not only in the courts of New Jersey but also at conferences in Geneva.

As I have written elsewhere, cyber insurance should be seen as a form of cyber diplomacy, as we aim to promote globally coordinated, nuanced, and effective regulation.

> If cyber diplomacy is truly concerned with enhancing cyber deterrence and promoting norms that ensure global cyber stability and cyber peace, it must broaden its perspective to include international insurance norms for modeling and indemnifying the perils of cyberspace.
>
> . . . .
>
> In an effort to expand the multi-stakeholder understanding of the risks cyber threats pose to society, we must begin to draw additional actors into the fold. Involving commercial reinsurers and insurers, brokers, underwriters, cyber risk insurance pool directors, corporate chief cyber risk officers, and insurance law and policy scholars and think-tanks in a larger conversation about the future of international cybersecurity would be a pivotal first step toward a more democratic and inclusive dialogue. Such a dialogue would offer more nuanced solutions to practical challenges, and would ensure better norm design by the very actors that will ultimately be tasked with ensuring the norms' proper implementation.[119]

---

[118] On December 6, 2021, the Superior Court of New Jersey granted Merck & Co.'s motion for partial summary judgment against Ace American Insurance Co. and denied the insurer's cross-motion. Merck & Co. v. Ace Am. Ins. Co., No. UUN-L-2682 at 8 (N.J. Super. Ct. Law Div. Dec. 6, 2021) (Bloomberg Law, Court Dockets). After examining both the plain language of the property insurance policy and the applicable caselaw surrounding the hostile/warlike exclusion, the Court concluded that the NotPetya cyberattack, allegedly launched by Russian officials, did not trigger the exclusion. *Id.* at 11. For a broader discussion of the topic and analysis of related attribution and international law matters see Scott J. Shackelford, *Wargames: Analyzing the Act of War Exclusion in Insurance Coverage and Its Implications for Cybersecurity Policy*, 23 YALE J. L. & TECH. 362 (2021).

[119] Lubin, *supra* note 109, at 24, 32 (footnotes omitted).

III. THE ROLE OF GOVERNMENT IN FOSTERING CYBER INSURANCE

With all this knowledge we may now come back to the question posed by the organizers of *A Cyber Cyber Insurance Conference*: what can, and should, state and federal governments do to promote more robust cyber insurance markets? To focus our analysis, let us look at one possible regulation: the recent New York Cyber Insurance Framework, the first of its kind in the country. The following section will assess the promise and limits of this framework and then offer broader observations about the future of cyber insurance regulation.

A. THE NEW YORK CYBER INSURANCE FRAMEWORK

On February 4, 2021, the New York Department of Financial Services ("NY DFS"), led by Superintendent Linda Lacewell, introduced the first state-wide cyber insurance regulation in the United States.[120] The circular, titled *Cyber Insurance Risk Framework*,[121] begins with a bombastic statement. Weaving together the impacts of COVID-19 on remote working, the rise of ransomware attacks, and the recent SolarWinds cyber-espionage campaign, it makes the case for such a state-wide intervention. The circular is thus meant to "foster the growth of a robust cyber insurance market that maintains the financial stability of insurers and protects insureds."[122]

The circular is the result of an "ongoing dialogue with the insurance industry and experts on cyber insurance," including meetings with "insurance regulators across the U.S. and Europe."[123] It identifies "systemic risk" and "silent risk" (what is known as non-affirmative cyber coverage) as two of the biggest challenges for managing cyber insurance, alongside the general challenge of dealing with the growing threat of cybercrime, in particular in the form of ransomware attacks.[124]

The framework applies only to "authorized property/casualty insurers [licensed in New York] that write cyber insurance."[125] The framework centers around seven practices that are to be employed by the

---

[120] Letter from Linda A. Lacewell, *supra* note 25.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.* (citing a 180% increase in ransomware insurance claims suggesting that ransomware is a $20 billion problem).

[125] *Id.*

insurers to "sustainably and effectively manage their cyber insurance risk."[126] The circular does note that each insurer's risk portfolio will vary on the basis of their "size, resources, geographic distribution, market share, and industries insured."[127] As such, the framework seems to offer a general and flexible model, subject to specific interpretation by each insurer. On the one hand, such flexibility allows for the kind of experimentation in regulation that I have argued is positive as the insured risks continue to evolve. On the other hand, such open-ended regulation could also result in a difficultly to enforce the standards, which could lower the regulation's overall effectiveness. The seven practices insurers should employ are:

> (1) "Establish a Formal Cyber Insurance Risk Strategy;"
> (2) "Manage and Eliminate Exposure to Silent Cyber Insurance Risk;"
> (3) "Evaluate Systemic Risk;"
> (4) "Rigorously Measure Insured Risk;"
> (5) "Educate Insureds and Insurance Producers;"
> (6) "Obtain Cybersecurity Expertise;" and
> (7) "Require Notice to Law Enforcement".[128]

There is obviously a lot of good intention here. The NY DFS should be commended for taking such a bold initiative at a time where few government regulators and legislatures (be it local, state, or federal) seem keen to enter the fray. It also targets some really low-hanging fruit, by formalizing the need of insurers to establish a cyber insurance risk strategy, retain qualified personnel, and obtain cybersecurity expertise, including through the use of outside providers and vendors. As one commentator noted, these are "both obvious and eye opening."[129] If there were any cyber insurers who were still unaware of these basic requirements, the circular might serve as a much-needed wakeup call and could help "create new incentives and pre-incident programs."[130] To the very least the circular helps codify a certain set of industry practices and general standards, which by itself is an important contribution, one that could be mimicked by other state regulators.

---

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] Joshua Mooney, *Breaking Down New York's Department of Financial Services' New Cyber Insurance Framework*, KENNEDYS L. (Feb. 18, 2021), https://kennedyslaw.com/thought-leadership/article/breaking-down-new-york-s-department-of-financial-services-new-cyber-insurance-framework/.

[130] *Id.*

Nonetheless, the circular suffers from significant ambiguity and uncertainty, further demonstrating the limits of one state regulator's authority and power in tackling such a massive undertaking. Within the limits of this paper, I will demonstrate four core challenges with the current framework.

First, why focus only on "authorized property/casualty insurers that write cyber insurance?"[131] In so doing, the circular seems to neglect both those insurers who do not explicitly write cyber insurance, as well as other insurers outside the property/casualty world. All these insurers might still be engulfed by the challenges of silent cyber coverage, yet the policy seems to target a very limited group.[132] As I have demonstrated above, asking who should be regulated, and in what ways, is one of the first challenges for every assessor.

Second, the framework "can inspire competing reactions as it signals incoming mandates that hover on the horizon without offering much substance as to how to accomplish them."[133] Take, as one example, the issue of "systemic risk." The circular calls on insurers to assess this risk, even citing the specific concern of supply-chain attacks as a possible vector in this regard.[134] But the circular falls short of actually providing insurers with specific tools, resources, or even general frameworks to conduct such analysis. As we have already seen, systemic risk is one of the areas where state insurers are way over their heads. Similarly, requiring insurers to develop "qualitative and quantitative goals for risk"[135] as part of a cyber insurance risk strategy and calling on them to "obtain cybersecurity expertise"[136] does not mean much if the state is not also willing to assist those insurers who need it by providing actual resources, actuarial techniques, specific recommended security controls, and even subsidies to certain industries or public entities, to accomplish these efforts.[137]

---

[131] Letter from Linda A. Lacewell, *supra* note 25.

[132] Thanks to Kenneth S. Abraham for pointing out this concern during the *A Cyber Cyber Insurance Conference*.

[133] Mooney, *supra* note 129.

[134] Letter from Linda A. Lacewell, *supra* note 25.

[135] *Id.*

[136] *Id.*

[137] As it currently stands, most commercial insurers do not possess "conclusive data on the effectiveness of cybersecurity controls and practices" nor are they well positioned at this time to "acquire and maintain a level of technical knowledge and expertise to advise on control selection and implementation conditioned on specific entity's security posture." DEP'T HOMELAND SEC., ASSESSMENT OF THE CYBER INSURANCE MARKET 15 (2019), https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf.

Third, the circular's only specific requirement—that policyholders notify law enforcement for ransomware attacks[138]—is also a source of some confusion. As a general matter, this is a policy that I have advocated for and makes a great deal of sense.

> [L]aw enforcement cannot carry out their duties, if they are not being informed of the hacks in the first place. There is a growing trend in cyber insurance policies to allow for ransomware extortion payment indemnification without requiring the policy holder to first notify the police or the FBI of the ransom prior to seeking compensation. Insurers argue that making such a demand to policyholders would disincentivize them from acquiring the policy in the first place, as they are worried about potential reputational harms. This collective action problem is resulting in a race to the bottom where it is enough for one insurer to avoid a requirement of notifying the FBI, for all insurers to follow suit out of worry of losing business.[139]

Nonetheless, one state regulator cannot tackle a collective action problem like this alone. The race to the bottom will continue if outside the state of New York, a failure to notify will continue to be the norm. This is a matter better left to federal regulation, not state. The circular is also silent as to the entity to be notified or scope of notification.[140] The reality is that the state is unable to actually enforce disclosure to federal law enforcement, over which it has no authority, nor can it be certain that the notification will be picked up and effectively handled once transmitted. A notification policy is only as good as the enforcement action that flows from it. As for local and state law enforcement, they are certainly in no position to manage the threat of global cybercrime and cyberwarfare, thereby highlighting the futility of notifying them.

Finally, a fourth challenge with the circular concerns the obligation to "rigorously measure insured risk" by focusing on a "data-driven" plan and "third-party sources."[141] In so doing, NY DFS seems to be going all-in

---

[138] Letter from Linda A. Lacewell, *supra* note 25.

[139] *See* Lubin, *supra* note 11, at 53–54.

[140] Letter from Linda A. Lacewell, *supra* note 25 (encouraging cyber insurance policies to include a requirement for victims to notify law enforcement but does not specify what law enforcement).

[141] *Id.*

on an AI-driven big-data insurtech solution. But the regulator fails to provide an actual list of preferred technologies, service-providers, or vendors. It leaves to the insurers the decision of who to contract with and in what ways, without even providing them the most limited set of considerations. Not all insurtech products are created equal, and different solutions could be more or less effective. Furthermore, as discussed, "the accelerating evolution of AI and big data render proxy discrimination a fundamental threat to important goals of many, if not most, antidiscrimination regimes."[142] The state fails to even acknowledge the myriad of ways by which the use of these tools could result in inequality, bias, privacy intrusion, and prohibited discrimination.

B. THE FUTURE OF CYBER INSURANCE REGULATION

For cyber insurance regulation, we must think outside the box. We need to adopt agility in the way we conceptualize the very concept of regulation. Understanding that the regulator, the regulated, and the regulation, can take different forms and occur at different times, is pivotal in developing a comprehensive and collaborative response to the contemporary threats and perils of cyberspace.

While insurance is traditionally viewed as a state-regulated market, the subject matter being insured, "cybersecurity," is certainly not. Insurers and insurance regulators should adopt a more holistic understanding of protections in cyberspace, recognizing that it is a domain ripe for complex public-private partnerships across a range of environments and frameworks.[143] Lessons from decades of U.S. regulation of privacy and data protection through a patchwork of sectoral and state initiatives (as opposed to an omnibus model in Europe) have led many scholars to call for federal and centralized regulation.[144]

---

[142] Prince & Schwarcz, *supra* note 74, at 1300.

[143] *See generally* JEFFREY BAXTER ET AL., ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 9 (Joseph Mazzafro ed., 2009), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_AddressingCyber_WP.pdf (providing a "graphic and conceptual representation of a possible system for cyber security partnership"); Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467 (2017).

[144] *See, e.g.*, Daniel J. Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY: PRIV. + SEC. BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/; Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL

The same could be applied here, precisely because of the unique features of cybersecurity as an evolving threat and the information asymmetries that accompany it. As such, no one state can handle cybersecurity risk on its own, just like no one insurer can cover this risk, especially if a mega cyber catastrophe occurs. In fact, recent trends have demonstrated precisely how unlikely it is that states and the market could handle this on their own. In the face of "skyrocketing" cyberattacks, including ransomware, insurers have begun to increase prices for cyber insurance products and denying coverage unless stringent controls are put in place.[145] As a result of that the market for primary cyber insurance "is really drying up."[146] In the face of these market shifts, only the federal government can effectively respond to and help fill this growing cyber insurance gap. An effective cyber insurance regulation will thus harness the commitment and dedication of state officials in a broader campaign co-led by national governments and the private sector.

CONCLUSION

As Rudyard Kipling masterfully opined in his 1943 poem, *The Secret of Machines*, the touch of technology can on occasion "alter all created things."[147] Emerging and evolving technologies introduce unique risks, harms, and regulatory challenges at different phases throughout each technology's life cycle. Against this background, rule-prescribers and rule-appliers have both a regulatory toolkit and a set of discretionary choices to make about the timing, scope, and nature of both prospective and reactive regulation. Commercial insurers play an important role in this narrative, both as private regulators of the technology they insure, and as a lobbying force to government in the formation of new regulations.

This paper has tried to demonstrate that there is value in exploring insurance regulation for emerging technologies through the broader lens of

---

ON FOREIGN RELS.: DIGIT. & CYBERSPACE POL'Y PROGRAM (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection; Joanna Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource",* 93 S. CAL. L. REV. 99 (2019).

[145] Ian Smith, *Cyber Insurers Recoil as Ransomware Attacks 'Skyrocket'*, FIN. TIMES (June 2, 2021), https://www.ft.com/content/4f91c4e7-973b-4c1a-91c2-7742c3aa9922.

[146] *Id*. (quoting Graeme Newman, chief innovation officer of London-based insurance provider CFC).

[147] Rudyard Kipling, *The Secret of the Machines* (1943), *reprinted in* A CHOICE OF KIPLING'S VERSE 293, 294 (T.S. Eliot ed., 1973).

the law-and-technology literature. Law-and-technology scholars, who have mastered a comparative regulatory history of different technologies, in different locations, and at different times, might be able to teach us a thing or two about the way we should govern our technological insurance markets.

The reverse is, of course, also true. Law-and-technology scholars, by and large, focus much of their writing on the theory and practice of torts, contracts, property, criminal, constitutional, and administrative law. Rarely though, do these tech-minded academics engage in a deep dive into insurance. If we each step outside of our own silo and explore what the folks on the other side are writing and thinking about, we might be able to develop deeper and more nuanced insights.

RANSOMWARE: A DARWINIAN OPPORTUNITY FOR CYBER INSURANCE

ERIN KENNEALLY*

TABLE OF CONTENTS

I. TAKING A CUE FROM NATURE

Charles Darwin's survival of the fittest theory maintains that an organism's ability to adapt to changes in its environment and adjust

---

* Erin Kenneally is the Global Director of Cyber Insurance at SentinelOne, where she provides cyber risk strategic thought leadership and domain expertise, and leads cyber security and data-driven innovation for cyber insurance solutions. Kenneally was previously Director of Cyber Risk Strategy at Guidewire-Cyence; and served as Portfolio Manager in the Cyber Security Division for the U.S. Department of Homeland Security, Science & Technology Directorate. At the U.S. Department of Homeland Security, Kenneally directed nearly twenty projects across programs in cybersecurity research data infrastructure, privacy, cyber risk economics, and technology ethics. Kenneally also previously served as Technology-Law Specialist at the International Computer Science Institute (ICSI) and the Center for Internet Data Analysis (CAIDA) and Center for Evidence-based Security Research (CESR) at the U.C. San Diego. Kenneally also founded and is CEO of Elchemy, Inc. Kenneally is a licensed attorney specializing in information technology law, including privacy technology, cyber security, AI & autonomous systems ethics and legal risk, trusted data sharing & governance, technology policy, and emergent IT legal risks. She holds Juris Doctorate and Masters of Forensic Sciences degrees and is a graduate of Syracuse University and the George Washington University.

accordingly over time determines its survival success.[1] This process of adaptation at the heart of Darwinism is apropos for the cyber insurance industry amidst the selective pressures introduced by ransomware incidents and claims. This case study proffers adaptations to the changes wrought by ransomware in order to increase cyber insurance resiliency against this peril and prevent coverage extinction. These adaptations exist on a spectrum of controllability and speed of impact. This includes risk management guidance; mandatory ransomware incident disclosure regulation; security controls failure reporting; information security ("InfoSec") prevention and mitigation controls incentives; data-driven risk models; and cyber extortion policy reform.

Borrowing from adaptation theory, there are three potential outcomes for the cyber insurance industry from the "habitat changes" caused by ransomware incidents: (1) extinction; (2) habitat tracking, whereby an organism moves away from the newly dangerous habitat to one more familiar; or (3) genetic change.[2] Respectively, these translate to: (1) insolvency—meaning the forced retreat from the entire cyber line of business as a result of attempting to support demand growth at unreasonable costs—or a rating event;[3] (2) reversion to an environment similar to pre-ransomware pressures, which means either jettisoning ransomware coverage, or pricing premiums or limits in-line with carriers' ransomware risk uncertainty that may result in underserving the quality and quantity of market demands; or (3) evolving capabilities that enable cyber insurers to maintain profitability and/or achieve reasonable loss ratios (based on risk-model-informed capital reserves and risk selection and pricing) for indemnifying ransomware victims.

Cyber insurers are scrambling to wrap their arms around ransomware risk and domesticate this peril. The industry has seen

---

[1] CHARLES DARWIN, THE ORIGIN OF SPECIES BY MEANS OF NATURAL SELECTION (John Murray ed., 6th ed. 1882).

[2] Susan King, *What is Adaptation Theory?*, SCIENCING (Mar. 13, 2018), https://sciencing.com/adaptation-theory-5105998.html.

[3] To date, and based on the author's knowledge, ratings institutions have not lowered any cyber insurance company ratings due solely to cyber peril. A rating event could conceivably derive from losses that would materially affect capital reserves/liquidity, which is a key credit consideration, such as the case with Moody's downgrade of Equifax following its 2017 data breach. *See* Kevin Townsend, *Moody's Downgrades Equifax Outlook to Negative Over 2017 Data Breach*, SECURITYWEEK (May 23, 2019), https://www.securityweek.com/moodys-downgrades-equifax-outlook-negative-over-2017-data-breach.

appreciable jumps in frequency and cost of reported incidents and claims, payouts, and demands in the last several years. Notable statistics include:

- Ransomware attacks increased nearly 150% after remote work increased due to the Covid-19 pandemic;[4]
- Ransomware claims and the cost of payments jumped approximately 230% from 2018 to 2019;[5]
- Cyber extortion demands paid in 2019 were four times higher than the previous year;[6]
- Average ransomware payouts for U.S. businesses went through the roof between third quarter 2018 and second quarter 2020—from under $10,000 in the latter half of 2018 to more than $178,000 per event by the middle of 2020, with large enterprises averaging over $1 million;[7] and

---

[4] *Amid Covid-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted*, VMWARE: SEC. BLOG (Apr. 15, 2020), https://blogs.vmware.com/security/2020/04/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted.html.

[5] Ben Dyson, *Cyber Insurers Tighten Underwriting, Raise Prices as Ransomware Wave Hits*, S&P GLOB. MKT. INTEL. (Oct. 22, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-tighten-underwriting-raise-prices-as-ransomware-wave-hits-60829821; Barnaby Page, *Ransomware: A Perilous Price to Pay*, SENTINELONE: BLOG (Dec. 7, 2020), https://www.sentinelone.com/blog/ransomware-and-the-perils-of-paying/.

[6] Page, *supra* note 5.

[7] *See Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase,* COVEWARE (Aug. 3, 2020), https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report*;* PALO ALTO NETWORKS, RANSOMWARE THREAT REPORT 3 (2021), https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf ("The average ransom paid by organizations in the US, Canada, and Europe increased from US$115,123 in 2019 to $312,493 in 2020—a 171% year-over-year increase.").

- Ransomware claims have comprised up to 40% of some insurers' cyber books,[8] along with a putative 10% loss ratio increase due to ransomware in 2019.[9]

As a result, premiums have risen[10] and insurers have become more selective,[11] undoubtedly underserving the quality and quantity of coverage demands. Taking a cue from Darwin, the path forward lies in recognizing ransomware as the functional equivalent of a natural selection event, admitting the possible outcomes, and taking responsibility for the trajectory that assures adaptation. Simply put, ransomware is a clarion call for cyber insurance industry adaptation.

II. PACE LAYERING

The starting point in crafting the cyber insurance industry's path forward is understanding the changed cyber insurance habitat ushered in by ransomware. The flag markers that the habitat has changed include:

- Insufficient actuarial data (loss history) for pricing premiums and coverage loss limits;
- Lack of risk control efficacy and attack vector lessons-learned;
- Expanding delta between cybercrime loss and claims paid;

---

[8] COALITION, CYBER INSURANCE CLAIMS REPORT 9–10 (2021), https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf (noting that the claims frequency in the first half of 2020 was 41%).

[9] JON LAUX, CRAIG KERMAN & SAMMIE COAKLEY, US CYBER MARKET UPDATE: 2019 US CYBER INSURANCE PROFITS AND PERFORMANCE 4–5 (2020), https://aon.io/2020-us-cyber-market-update.

[10] *See, e.g.*, *id.* at 3; Page, *supra* note 5 (quoting Chris Keegan of Beecher Carlson, "[i]nsurance carrier [premium] increases of zero to five percent rate in the second quarter 2020, gave way to five to fifteen percent increases in the third quarter which were raised again to ten to thirty percent in the fourth quarter. Not all increases are in this range, but cyber insurance buyers should be prepared for requests at these levels. Some adjustments to the structure of programs, such as raising retentions, can be made to limit the increased costs and carriers are amenable to these discussions.").

[11] Page, *supra* note 5 (quoting Chris Keegan of Beecher Carlson, "[i]n addition, insurers are focusing on more careful selection of their policyholders.").

- A gap in spending between cyber security and risk transfer;
- Uncomfortable ransomware loss ratio distributions;
- Premiums that are more sensitive to market competition rather than organizations' security posture and perceived ransomware threat; and
- Incongruency between threat capabilities and modeled risk profiles, including loss accumulation potential.[12]

The next step in the process of crafting a path forward is assessing and identifying the adaptations—change agents—that will put cyber insurers on the path to survival regarding ransomware coverage. Enter "pace layering," a framework for diagnosing and prescribing how adaptable an entity[13] is to change.[14] Pace layering proposes that every entity is the product of adaptation to the demands of six-time scales that move and change at different paces.[15] Ordered from slow to fast, these are nature, culture, governance, infrastructure, commerce, and aesthetics (e.g., art and fashion).[16] The slower layers are thought of as lower, more foundational and methodical, but provide stability.[17] The fast layers are more innovative and less encumbered, but also less stable.[18] For example, in a healthy, strong society our legal systems change slower than the rate of commerce, throttling the rate of change in a society to enable social normative grounding. As pace layering's framer, Stewart Brand, notes, "[f]ast gets all our attention, but slow has all the power."[19]

---

[12] *See generally* Ben Dyson, *Cyberrisk Models Advance Quickly, but Still Lag Natural Catastrophe Reliability*, S&P GLOB. (Dec. 30, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyberrisk-models-advance-quickly-but-still-lag-natural-catastrophe-reliability-61766574.

[13] An umbrella term used here to represent a system, organism, or organization.

[14] Stewart Brand, *Pace Layering: How Complex Systems Learn and Keep Learning*, J. DESIGN & SCI. (Feb. 4, 2018, 2:45 PM), https://jods.mitpress.mit.edu/pub/issue3-brand/release/2.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

Each layer interplays with the others to adapt to change in different ways, with the continuity of all the layers determining survival.[20] When faster layers move too slowly, the entity may become stagnant as it seeks to recover from its fast growth, or have cultural level misalignment.[21] Conversely, faster layers (e.g., commerce) can move too quickly for what infrastructure and culture can support, causing a system breakdown.[22] Similarly, when slower layers move too quickly, they can cause turmoil, whereas, if they move too slowly, they impede progress at higher layers.[23]

The 1906 San Francisco earthquake is relevant and illustrative of how pace layering can explain the mid- and higher-layer adaptations required to recover from abrupt changes at the lowest layer. The earthquake led to "a rapid change in nature [which] sent a shockwave all the way up to the commerce layer, destroying the city infrastructure, bankrupting businesses and households, and requiring governance to step in and subsidize the recovery."[24] The financial infrastructure could not absorb the shocks that were unbuffered by an insurance industry that was unable to underwrite damage on such a large scale, and the market panicked a year later.[25]

Autonomous vehicles are a more current example where change introduced at the fast layers exposes tensions at slower layers. At the commerce layer, auto manufacturers have mobilized quickly, moored by a relatively mature infrastructure.[26] But legal (e.g., governance) and ethical (e.g., culture) layers flounder when comes to assigning responsibility for the inevitable "trolley dilemma", where car driven by artificial intelligence is put in a position to make a choice to save the driver and plunge into a crowd or sacrifice the driver for the sake of bystanders.[27]

---

[20] *Id.*

[21] Jonathan Maricle, *Pace Layering: An Application Strategy for Resilient Products*, PURPLE, ROCK, SCISSORS: BLOG (Oct. 11, 2018), https://purplerockscissors.com/blog/pace-layering-application-strategy.

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *The San Francisco Earthquake of 1906: An Insurance Perspective,* INS. INFO. INST., https://www.iii.org/article/san-francisco-earthquake-1906-insurance-perspective (last visited Dec. 30, 2021) ("Of the $235 million in insured losses, only about $180 million was paid out in claims as many financially-strapped insurers could pay only a share of the actual losses.").

[26] Maricle, *supra* note 21.

[27] *Id.*

III. RANSOMEWARE ADAPTATIONS

We can apply the pace layering framework to diagnose and recommend adaptations to the current ransomware insurance challenges by answering the following three key questions.

1. In which layer(s) are ransomware impacts most felt?

Ransomware impacts have been felt most immediately through selective pressures at the commerce layer. Following the title of Jim Carrey's cult 1994 movie, *Dumb & Dumber,*[28] insurance companies have been throwing dumb capacity at the fast-growing commerce layer and dumber risk management at the infrastructure layer.[29] This emergence has been accelerated by the digital revolution of cryptocurrency technology, which has enabled a less risky and faster pay-out for attackers.[30] The industry is now struggling to absorb the commodification of ransomware coverage in response to dynamic ransomware threat trends and concomitant commoditization of attacks.[31] In short, there has been a disconnect between the actual risk and how it was priced in premiums. While this peril is not novel, carriers in the previous, longstanding soft cyber market with healthy reserves and capacity continued to write ransomware policies (albeit more selectively or with higher premiums) without the necessary supporting

---

[28] DUMB & DUMBER (New Line Cinema 1994).

[29] *See* Ryan Smith, *Cyber Insurance Market Continues to Accelerate*, INS. BUS. MAG.: AM. (May 11, 2018), https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurance-market-continues-to-accelerate-100346.aspx ("'As cyber underwriting exposure grows, more cyber incidents will be covered, generating claims that lead to weaker underwriting results,' said Gerry Glombicki, director at Finch. 'From an individual underwriter perspective, the risk of naïve capacity entering the market, growing rapidly without sufficient expertise and ultimately suffering outsized losses in cyber is an expanding possibility.'").

[30] *See* GUIDEWIRE-CYENCE, TAMING THE UNCERTAINTY OF RANSOMWARE RISK 4–5 (2020), https://success.guidewire.com/rs/140-LHX-683/images/WP_RansomwareInsights_June2020.pdf.

[31] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 19 (2021), https://www.gao.gov/assets/gao-21-477.pdf ("[E]ven as insurers collect more data and hone predictive models based on prior cyber threats, the underlying exposure keeps changing. This makes it difficult to create a reliable predictive model when it is not clear what new objective, strategy, or technique cyber threat actors may deploy.").

infrastructure needed to inform pricing and selection adjustments to the risk.[32]

2. Out of which layer(s) did the ransomware challenge emerge?

While the ransomware selective pressure has been felt most immediately at the commerce layer, it stemmed from inadequate growth at the governance and infrastructure layers. This tension has built up over the past five-plus years of expanded underwriting for this peril, without commensurate progress at the infrastructure and governance layers of cyber insurance that are needed to mitigate the balance sheet/loss ratio shocks that are now felt at the commerce layer.[33] These infrastructure deficiencies include the lack of policies and processes to bring about sufficient security risk management coordination or implementation incentives, learned knowledge of the efficacy of security controls in the face of specific incidents, and risk models that are informed by critical data and expert knowledge.[34]

3. From which layer(s) is a solution most likely to emerge?

The answer here includes multiple entities responding at multiple layers.[35] Ransomware challenges are best addressed by introducing adaptations[36] at the cyber insurance's cultural and governance layers,[37] and ultimately effectuated at the infrastructure and commerce layers. The

---

[32] *See id.* at 13–14 (noting that limited historical data on cyber losses makes pricing and quantifying risk difficult).

[33] *See id.* at 8–13; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., ASSESSMENT OF THE CYBER INSURANCE MARKET 9–10 (2019), https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf.

[34] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 31, at 17–26; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 33, at 2–17.

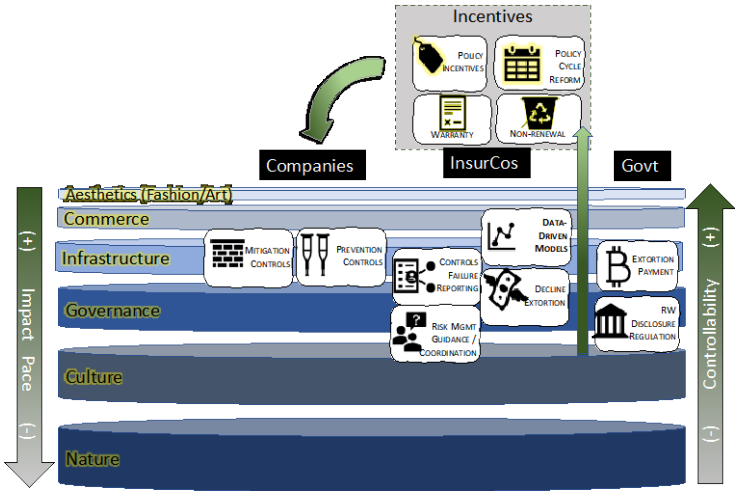
[35] *See infra* Figure 1.

[36] *See* adaptations discussion *infra* Section IV.

[37] In order to effectuate the adaptation, carriers need to embrace their role as stewards of risk management (see Figure 1) and thereby require/incentivize implementation of cyber security controls to prevent and mitigate loss. This is juxtaposed to what they've historically done which is look to another institution (i.e., government and case law) to be that forcing function for selection and implementation of security controls.

adaptations introduced at the infrastructure, governance, and culture layers are the core of the Darwinian path forward for cyber insurance and ransomware.

Figure 1: Layers of Ransomware Insurance Adaptations



IV. ADAPTATIONS–THE PATH FORWARD

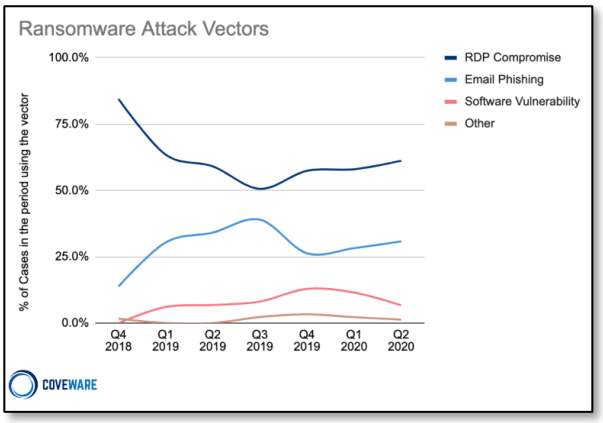
The rest of this paper explores in more detail the specific adaptions and necessary incentives to create a stable response to the ransomware risk.

A. INFOSEC LOSS PREVENTION AND MITIGATION CONTROLS

While the progress on gaining the necessary ransomware actuarial data leaves much to be desired, InfoSec statistics around the threat and vulnerability dimensions of risk have improved and show remarkable consistency in the case of ransomware. Reports from leading vendors assert that the most popular attack vectors and sources of ransomware incidents are

Remote Desktop Protocol ("RDP"),[38] email phishing ("SPAM"), and unpatched vulnerabilities.[39]

Figure 2: Common Ransomware Attack Vectors[40]



Knowing where to spend limited cyber security budgets can be challenging—especially in what some would refer to as a market for lemons, where product and service efficacy benchmarks are lacking, and successful attacks often exploit the human-technology interface gaps.[41] There are nonetheless "known-knowns," which involve basic blocking and tackling that can significantly decrease risk exposures. These known-knowns include: ensuring that RDP ports and services are not openly exposed to the internet; maintaining updated software patches for virtual private networks (VPN) and appliances that provide entryways to corporate networks; implementing

---

[38] For a description of RDP see Jareth, *How to Secure RDP From Ransomware Attacks*, EMSISOFT: BLOG (July 20, 2020), https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/.

[39] *See* RECORDED FUTURE, PULSE REPORT: ANALYZING THE THREAT OF RANSOMWARE ATTACKS AGAINST US ELECTIONS 7–9 (Allan Liska ed., 2020), https://go.recordedfuture.com/hubfs/reports/cta-2020-0820.pdf; Jareth, *supra* note 38; *Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, supra* note 7. *See also infra* Figure 2.

[40] *Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, supra* note 7.

[41] *See* Daniel W. Woods & Tyler Moore, *Cyber Warranties: Market Fix or Marketing Trick?,* 63 COMMC'NS ASS'N FOR COMPUTING MACH. 104 (2020).

endpoint detection, protection, and response (EDR); applying email fraud/social engineering controls; and enforcing multifactor authentication (MFA) and privilege access management (PAM) to harden IdAM (identity and access management).[42] These risk prevention controls are the direct responsibility of corporate policyholders, yet cyber carriers on the whole have done little to incentivize their adoption.[43]

In addition to prevention controls, arguably the closest thing to an InfoSec silver bullet for ransomware mitigation is backup recovery technology. Since locking systems and extorting payments in exchange for decryption keys is the trademark of ransomware, effective backups are its strongest antibody.[44] Indeed, implementation complexity, costs, and associated business continuity implications are not monolithic and can be complicated.[45] Yet, the difference between quick and local backups[46] and ransomware-resistant backups[47] is that the former may involve weeks of

---

[42] *See, e.g.*, Marisa Midler, *3 Ransomware Defense Strategies*, SOFTWARE ENG'G INST.: BLOG (Nov. 9, 2020), https://insights.sei.cmu.edu/blog/3-ransomware-defense-strategies/; *Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase*, *supra* note 7; Perry Carpenter, *5 Defenses for 5 Ransomware Root Causes*, CPO MAG. (Dec. 6, 2021), https://www.cpomagazine.com/cyber-security/5-defenses-for-5-ransomware-root-causes/.

[43] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 31, at 17 ("NAIC representatives told us the industry may offer additional cyber services to help policyholders manage their cyber risk. But they added that some small and mid-size businesses have limited technical resources or staff with cybersecurity expertise and are not taking full advantage of these services."); Shauhin A. Talesh & 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. 967, 1003–04 (2021) (discussing pre- and post-breach services insurers provide their insureds but do not require them to use in order to get premium discounts or to qualify for coverage).

[44] *See* Emily Heaslip, *What Small Businesses Need to Know About Ransomware*, U.S. CHAMBER OF COM. (June 9, 2021), https://www.uschamber.com/co/run/technology/small-businesses-ransomware.

[45] *See Data Backup and Disaster Recovery*, ONTECH SYS., INC., https://ontech.com/data-backup-disaster-recovery/ (last visited Jan. 2, 2022).

[46] For example, simply keeping an archived copy of data.

[47] Best practices include the 3-2-1 Rule: keeping three backups on two different types of media with one of which being offsite; securing data using industry standard encryption, and regularly testing to ensure data accuracy and recoverability. *See*

downtime due to failed and insufficient recoverability and six to seven figure business interruption, whereas the latter may involve days of downtime and lower upfront cost.[48] Some statistics reveal that sixty percent of company backups are incomplete and fifty percent of restores fail.[49] This has resulted in insurers opting to pay ransoms as a result of cost-benefit analyses that find the business interruption costs associated with recovery and restoration from backups to be more painful than coughing up the extortion fees and hoping that attackers will honor their word.[50] The pink elephant question is, why then are insurers not insisting on provably robust disaster recovery technologies and processes as a precondition to coverage?

Ransomware is exposing cracks in the cyber resilience of both cyber insurers and victim organizations. More significantly, it lays bare the gap between the two, the closure of which is key to improving resilience for sets of stakeholders. Organizations targeted by ransomware are ultimately the ones in control of implementing prevention and mitigation controls, yet economic, talent, and governance deficiencies leave them unattended in many companies.[51] As transferors of financial risk from victim companies,

---

PETER KROGH, THE DAM BOOK: DIGITAL ASSET MANAGEMENT FOR PHOTOGRAPHERS 88 (Colleen Wheeler ed., 2nd ed. 2006).

[48] *See 4 Data Recovery Solutions for Small Businesses*, ONTECH SYS. INC., https://ontech.com/data-recovery-solutions/ (last visited Jan. 2, 2022).

[49] *5 Shocking Statistics About Data Backup and Recovery*, ONTECH SYS. INC., https://ontech.com/data-backup-statistics/ (last visited Jan. 2, 2022).

[50] *See* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

[51] *See* Ariel E. Levite, Scott Kannry & Wyatt Hoffman, *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance* 24 (Carnegie Endowment for Int'l Peace, Working Paper Oct. 2018), https://carnegieendowment.org/files/Cyber_Insurance_Formatted_FINAL_WEB.PDF (discussing the "perverse incentive structure[s] for many industries" and how it leads to the problems currently faced in cyber security); *The Role of Cyber Insurance in Risk Management: Hearing Before the S. Comm. on Cybersecurity, Infrastructure Prot., & Sec. Techs. of the Comm. on Homeland Sec.*, 114th Cong. (2016), https://www.govinfo.gov/content/pkg/CHRG-114hhrg22625/html/CHRG-114hhrg22625.htm [hereinafter *The Role of Cyber Insurance in Risk Management*]. *See generally* OECD, ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT 14, 74–77 (2017), https://www.oecd.org/daf/fin/insurance/

insurers are in a position to indirectly bring about these infrastructural changes by wielding various incentives to improve the cyber hygiene that can significantly impact ransomware loss.[52] Properly structured, the following incentives can be a behavioral-forcing function to reduce ransomware risk:

- Refuse to bind/renew companies who cannot attest to having these controls in place;[53]
- Institute premium reductions for those that have a clean exposure signal (e.g., open RDP) bill of health;[54]
- Change policy cycles to be more agile and responsive to cyber exposures;[55]
- Issue cyber warranty[56] for security vendors to enhance trust in efficacy claims;[57]

Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf (discussing that while companies are in control of their security procedures, insurance companies can help in various ways due to their expertise).

[52] *See* Levite, Kannry & Hoffman, *supra* note 51, at 20–21; *The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51, at 74–77; Letter from Linda A. Lacewell, Superintendent, N.Y. State: Dep't Fin. Servs., to All Authorized Prop./Cas. Insurers (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02; DANIEL M. HOFMANN, ADVANCING ACCUMULATION RISK MANAGEMENT IN CYBER INSURANCE: PREREQUISITES FOR THE DEVELOPMENT OF SUSTAINABLE CYBER RISK INSURANCE MARKET (2019), https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/research_brief_advancing_accumulation_risk_management_in_cyber_insurance.pdf.

[53] *See* Levite, Kannry & Hoffman, *supra* note 51, at 18 ("Third-party expert assessments of a policyholder's assets would give insurers greater insight and understanding of risk exposure. More important, these practices would directly raise the baseline level of security by identifying flaws and motivating efforts to mitigate them by making coverage conditional upon their being addressed."); *The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51, at 74.

[54] OECD, *supra* note 51, at 14–15 (noting premiums may also be reduced if policyholder seeks to reduce its risks by investing in better cyber security).

[55] *See generally The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51.

[56] Cyber warranty covers the cost to remediate and update a vendor's client system in the event its product and/or services are the cause of a cyber peril. *See* Woods & Moore, *supra* note 41, at 105–06.

[57] Arguably warranties may not incentivize controls investment, rather they prevent vendors from overexaggerating the functionality of products. *See id.* at 106.

- Policy cancellation or amendment of terms and conditions mid-policy if an insured neglects recommended security improvements.[58]

B. RISK MANAGEMENT COORDINATION

Incentivizing ransomware risk controls is a necessary but insufficient adaptation at the commerce layer if insurers want to withstand the dynamic, evolving risk that is ransomware. Unless incentives are intertwined with infrastructure layer security metrics, the prescribed controls will invariably lag behind threats and vulnerabilities. As well there will also be continued conceptual misalignment between the ransomware coverage (insured risk) and ground-up risk, which is a recipe for coverage blind spots and market mistrust when claims are denied.[59] Rather than relying primarily on exogenous factors like compliance or glacially-paced case law[60] to define risk, embracing a risk management coordination role enables cyber insurers to proactively address losses closer to where they are felt and take the fight to ransomware.[61] Security risk metrics coordination "between underwriters, brokers, and [I]nfo[S]ec professionals can better align risk optics, lower information asymmetries, and scale victimology beyond the current ad hoc

---

[58] *See* Levite, Kannry & Hoffman, *supra* note 51, at 20–21; *The Role of Cyber Insurance in Risk Management*, *supra* note 51; OECD, *supra* note 51, at 74.

[59] *See* OECD, *supra* note 51, at 8–9 (discussing insured's level of uncertainty over cyber insurance coverage); Levite, Kannry & Hoffman, *supra* note 51, at 18–19 (arguing for "[c]ontract simplicity and understanding.").

[60] *See* ANDREW GRANATO & ANDY POLACEK, FED. RSRV. BANK OF CHI., CHI. FED LETTER NO. 426, THE GROWTH AND CHALLENGES OF CYBER INSURANCE 4 (2019) ("This [legal] uncertainty standing in data breach litigation . . . directly affects the probability that an insurer will have to pay claims in the event of a data breach and this, in turn, affects how they should price their insurance policies."); U.S. DEP'T OF HOMELAND SEC., CYBER RISK ECONOMICS CAPABILITY GAPS RESEARCH STRATEGY 13, 16–17, 20 (2018), https://www.dhs.gov/sites/default/files/publications/3950_CYRIE_Report_FINAL508.pdf [hereinafter CYRIE REPORT].

[61] *See, e.g.*, Richard S. Betterley, *Cyber/Privacy Insurance Market Survey*, BETTERLEY REP., June 2015, at 13–14. Robust underwriting of cyber insurance coverage can contribute to reducing cyber risk at an aggregate level by disseminating and ensuring compliance with good security practices–similar to the market for large commercial property coverage where insurance companies play a valuable risk consulting role. *See id.* at 7; OECD, *supra* note 51, at 73–75.

dynamics."[62] Insurance companies have thus far formed partnerships with InfoSec organizations for post-event response and consulting.[63] What is needed now is synchronization with the InfoSec consortium and other organizations for prevention and mitigation measures and advisement.

Several notable statistics shed light on this coordination gap.[64] First, is the ratio between the economic cost of cybercrime and claim payouts, which was estimated to be less than one percent in 2016.[65] The difference between cybercrime costs and insurance premiums, estimated to be $695 billion, can serve as a similar proxy.[66] Similarly, the disparity between cybersecurity spending and insurance premiums is estimated to be $116 billion.[67] Global cyber insurance expenditures and risk transfers are growing at slower rates than overall InfoSec spending and cybercrime losses.[68] These

---

[62] Erin Kenneally, *Ways Insurers Can Reduce the Threat of Cyber Risks*, NU PROP. & CAS. (Feb. 4, 2022, 5:00 AM), https://www.propertycasualty360.com/2022/02/04/ways-insurers-can-reduce-the-threat-of-cyber-risks/. *See also* OECD, *supra* note 51, at 14.

[63] THE COUNCIL OF INSURANCE AGENTS & BROKERS, CYBER INSURANCE MARKET WATCH SURVEY: EXECUTIVE SUMMARY 7 (6th 2018), https://www.ciab.com/download/15077/.

[64] *See infra* Figures 3 and 4.

[65] The White House Counsel of Economic Advisors estimated the economic cost of cybercrime to be between $57 billion to $109 billion in 2016. COUNCIL OF ECONOMIC ADVISERS, EXECUTIVE OFFICE OF THE PRESIDENT, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 36 (2018), https://www.hsdl.org/?view&did=808776. "During that same period, U.S. insurance companies incurred $356 million in claims from policyholders, equivalent to less than 1% of estimated losses. Compare this to natural catastrophes, where 50% of losses between 2015 and 2018 were paid by insurers." GRANATO & POLACEK, *supra* note 60, at 5 (footnotes omitted). This information was "[b]ased on insurance statutory filings from S&P Global Market Intelligence. Data include both standalone and packaged policies, but not claims paid by surplus line insurers that are not required to report financials to the NAIC." *Id.* at 5 n.13.

[66] Manuel Adam & Simon Ashworth, *Cyber Risk in a New Era: Insurers Can be Part of the Solution*, S&P GLOB. RATINGS (Sept. 2, 2020, 11:43 AM), https://www.spglobal.com/ratings/en/research/articles/200902-cyber-risk-in-a-new-era-insurers-can-be-part-of-the-solution-11590046 (comparing the estimated $5 billion in commercial and private cyber insurance premiums to the estimated $700 billion for yearly economic costs of cybercrime). *See also infra* Figure 3.

[67] *See infra* Figure 4.

[68] *See* Adam & Ashworth, *supra* note 66; Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.

two trajectories signal the current incongruity between what should be a symbiotic relationship, as well as an underserved opportunity for cyber insurers.

Figure 3: Annual Cyber Security and Cyber Insurance Spending Worldwide[69]

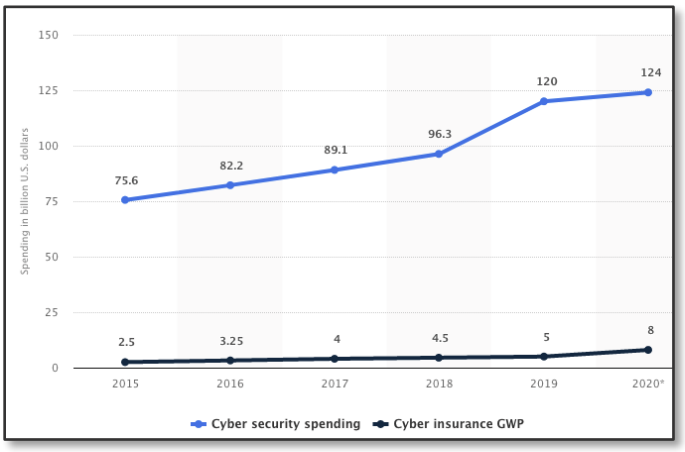
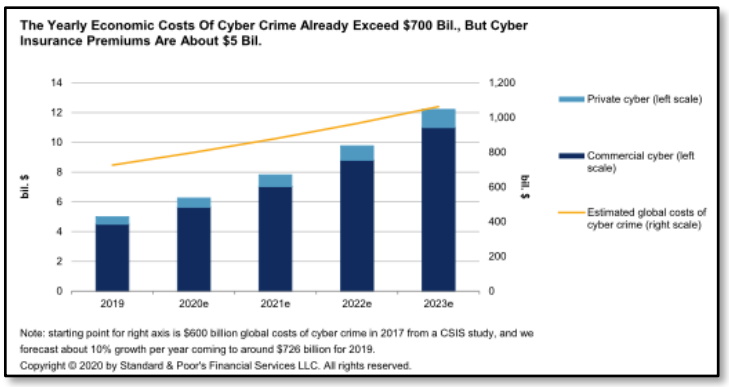


Figure 4: Cost Trend of Cyber Crime v. Cyber Insurance Premiums[70]



[69] Joseph Johnson, *Global Cyber Security & Cyber Insurance Spending 2015-2020,* STATISTICA (Jan. 25, 2021), https://www.statista.com/statistics/387868/it-cyber-securiy-budget/.

[70] Adam & Ashworth, *supra* note 66.

How the risk management coordination mantle can be taken up by cyber insurers lies on a spectrum. At a basic level, simply requiring policyholders/applicants to provide or verify fundamental firmographics and technographics (e.g., company domain name, subdomain ownership) for accurate cyber risk assessment is a trivial lift. On the other end of the spectrum, incentivizing insureds to share internal security telematics is a known missing link in cyber risk understanding.[71] While contribution of inside-the-firewall security data would require some technical, procedural, and policy changes on the part of the insured and insurer, incorporating this telemetry it would be a game changer for cyber risk insurance.

C. RANSOMWARE DISCLOSURE REGULATION

Since, arguably, industry-specific federal regulation, litigation, and state laws requiring reporting and disclosure of data breaches[72] drove the actuarial foundation upon which data breach coverage is anchored, it begs asking do we need a similar forcing function in order to adapt to ransomware risk? Regulatory fines, reporting requirements, liability and legal costs made data privacy and insecurity losses tangible and manifest, thereby capturing the attention of the industry.[73] This regulatory impetus fed the rational expectation that improved cybersecurity would result in reduced premiums and/or higher liability limits.[74]

As more ransomware attacks hybridize to exfiltrate and hold data hostage to pressure extortion payments, many of the existing public

---

[71] *See* OECD, *supra* note 51, at 96; JAMIE MACCOLL, JASON R C NURSE & JAMES SULLIVAN, CYBER INSURANCE AND THE CYBER SECURITY CHALLENGE 29–30 (2021), https://static.rusi.org/247-op-cyber-insurance-fwv.pdf.

[72] *See* CYRIE REPORT, *supra* note 60, at 20.

[73] *Special Report: Cyber Insurance Market: Stress Testing the Future*, BEST'S REV. (Oct. 2018), https://news.ambest.com/articlecontent.aspx?pc=1009&refnum=278309 ("The U.S. cyber insurance market took off as data breach notice and other privacy laws were implemented which highlights the tangible costs associated with data breaches.").

[74] *See* THE COUNCIL OF INS. AGENTS & BROKERS, CYBER INSURANCE MARKET WATCH SURVEY EXECUTIVE SUMMARY 7 (3rd ed. 2016), https://www.ciab.com/wp-content/uploads/2017/04/102016CyberSurvey_Final.pdf; THE COUNCIL OF INS. AGENTS & BROKERS, CYBER INSURANCE MARKET WATCH SURVEY EXECUTIVE SUMMARY 3 (2nd ed. 2016), https://www.ciab.com/wp-content/uploads/2017/04/2ndCyberMarketWatch_ExecutiveSummary_FINAL.pdf; THE COUNCIL OF INS. AGENTS & BROKERS, *supra* note 63, at 7–8.

disclosure requirements (and privacy claims) will be triggered.[75] Yet it is very much an open question as to whether that will be sufficient for robust underwriting of ransomware risk. At present, the industry has an inadequate understanding of ransomware risk distributions to select risks and underwrite policies proportional to reserves and risk appetite, while still being responsive to the needs of the market.[76] In any case, the government is uniquely situated to control for this adaptation.

D. CONTROL FAILURE REPORTING

The adage, "to not know history is to be doomed to repeat it"[77] is sage advice for ransomware adaptation. Standard components of cyber incident digital forensics and incident response ("DFIR") reporting include information about attack vectors and control failures, which is to say, how attackers were able to access company networks and what technical or administrative safeguards were deficient.[78] While the certainty of these attributions varies, insurers have by and large left these ransomware claims artifacts on the cutting room floor, foregoing valuable lessons-learned and

---

[75] For example, entities covered by Health Insurance Portability and Accountability Act ("HIPAA") that are infected with ransomware are presumed to have a reportable data breach unless it can be shown that there was a low probability that the protected health information ("PHI") has been compromised. Off. for Civ. Rts., *Breach Notification Rule*, HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. S*ee also* Yotam Gutman, *The Stopwatch Is Ticking | How Ransomware Can Set a Breach Notification in Motion*, SENTINELONE: BLOG (June 1, 2020), https://www.sentinelone.com/blog/the-stopwatch-is-ticking-how-ransomware-can-set-a-breach-notification-in-motion/.

[76] MACCOLL, NURSE & SULLIVAN, *supra* note 71, at vii.

[77] *See History Repeating*, VA. TECH COLL. OF LIBERAL ARTS & HUM. SCIS., https://liberalarts.vt.edu/magazine/2017/history-repeating.html (last visited Mar. 1, 2022) ("Spanish philosopher George Santayana is credited with the aphorism, "[t]hose who cannot remember the past are condemned to repeat it . . . .").

[78] *See Digital Forensics and Incident Response (DFIR)*, CROWDSTRIKE (July 1, 2021), https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/; Stephen Watts, *Digital Forensics and Incidental Response (DFIR): An Introduction*, BMC (Feb. 13, 2020), https://blogs.bmc.com/dfir-digital-forensics-incident-response/?print-posts=pdf.

helping perpetuate underwriting whack-a-mole.[79] Imagine if, over the course of the last decade of claims, individual insurers, or better yet, the collective industry, had documented these DFIR or security audit data points as part of the claims process. While there is no guarantee that the past is prologue when it comes to cyber risk, attacker tactics, techniques, and practices ("TTPs") follow patterns and paths of least resistance, and knowing their playbooks goes a long way towards reducing exposures.[80]

Concerningly, there is a trend with insurers—mostly in the small and medium-sized enterprises ("SME") market—cutting costs by collecting less information during the underwriting process and eliminating data fields in the notification of loss.[81] This trend works counter to the below-suggested adaptation aimed at developing more mature and validated cyber loss models to align the underwritten risk with price premiums.[82]

Adaptation within a dynamic cyber risk landscape and a market of proliferating security widgets and services whose efficacy is hard to differentiate, requires committing this data to the actuarial record. Collecting and sharing controls failure data would mark a significant step toward being

---

[79] *See generally* ERIN KENNEALLY, HIDING IN PLAIN SIGHT: TOWARDS NOW-GEN CYBER RISK UNDERWRITING (2021), https://success.guidewire.com/Whitepaper-HidinginPlainSightTowardsNow-GenCyberRiskUnderwriting_Registration.html; Daniel W. Woods & Rainer Böhme, *How Cyber Insurance Shapes Incident Response: A Mixed Methods Study,* 20 WORKSHOP ON ECONS. INFO. SEC. (2021), https://informationsecurity.uibk.ac.at/pdfs/DW2021_HowInsuranceShapes_WEIS.pdf.

[80] Ken Dunham & Christopher Lucas, *TTPs Within Cyber Threat Intelligence,* OPTIV (Jan. 19, 2017), https://www.optiv.com/explore-optiv-insights/blog/tactics-techniques-and-procedures-ttps-within-cyber-threat-intelligence.

[81] *See* PWC, TOP ISSUES: SHIFTING COST CURVES TO STAY IN THE COMMERCIAL INSURANCE RACE 4–5 (2018), https://www.pwc.se/sv/pdf-reports/forsakring/insurance-top-issues-2018-commercial-cost-curve.pdf (noting seventy-five percent of insurers have implemented costs cutting programs, which may include reducing information gathering in the underwriting process). PWC, ARE INSURERS ADEQUATELY BALANCING RISK & OPPORTUNITY? FINDINGS FROM PWC'S GLOBAL CYBER INSURANCE SURVEY (2018), https://cyber-liability.org/reports/pwc-cyber-insurance-survey.pdf.

[82] *See, e.g.*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., ASSESSMENT OF THE CYBER INSURANCE MARKET 13 (2018), https://www.cisa.gov/sites/default/files/publications/20_0210_cisa_oce_cyber_insurance_market_assessment.pdf [hereinafter CISA REPORT].

able to qualify and quantify the end-to-end relationships between threats, security compliance, and incident outcomes.[83]

E. DATA-DRIVEN MODELS

Because ransomware is a dynamic threat whose prevalence is unknown, and because it operates within interconnected target landscapes, knowledge of yesterday's attacks is insufficient to inform us about tomorrow's outcomes.[84] Cyber foresight is, therefore, a prerequisite for effective ransomware risk segmentation, assessment, pricing, and defense. Foresight comes by way of predictive models that include both historical data and expert knowledge.[85] Simply fitting historical event frequency and severity distributions around ransomware event variables and parameters that appear to conform with what the market thinks is accurate, will not anticipate the future changes that are endemic to this risk.[86] The adaptation needed is empirical data-driven ransomware models which incorporate expert knowledge and that validate over time against actual results.[87] The end game is validated; predictive models that drive more robust and reliable pricing models and inform underwriting guidelines.

Models can be validated by measuring the difference between the predicted and observed outcomes.[88] This is typically done using historical data only, with ongoing monitoring of the actual results being a secondary consideration that is too often ignored.[89] But in an actively changing environment, historical results often lack necessary information for predicting the future, meaning that a model whose output agrees with

---

[83] *See id.* at 14; CYRIE REPORT, supra note 60, at 29–31.

[84] *See* MACCOL, NURSE & SULLIVAN, *supra* note 71, at 31.

[85] *See* Venkatesh Jaganathan, Priyesh Cherurveettil & Premapriya Muthu Sivashanmugan, *Using a Prediction Model to Manage Cyber Security Threats*, 2015 SCI. WORLD J. (SECURITY OF INFORMATION AND NETWORKS SPECIAL ISSUE) 1, 4 (2015), https://downloads.hindawi.com/journals/tswj/2015/703713.pdf.

[86] *See* MACCOL, NURSE & SULLIVAN, *supra* note 71, at 31.

[87] *See* Jaganathan, Cheruvreettil & Sivashanmugan, *supra* note 85, at 4.

[88] *See* Chris Cooksey, *Guidewire's Approach to Predictive Analytics, Part Five: Monitoring*, GUIDEWIRE (Oct. 23, 2020), https://www.guidewire.com/blog/technology/guidewires-approach-predictive-analytics-part-five-monitoring/.

[89] Correspondence with Chris Cooksey, Head Actuary, Guidewire Analytics (Jan. 2021). *See id.* ("Any predictive model on which a business process depends must be monitored for effectiveness.").

observed historical behavior (a validated model) may be inaccurate in the future.[90] At the same time, if the predictive model is created as a blend of data-driven historical patterns and expert knowledge, it can only truly be validated against the future that will manifest over time.[91] So, optimal validation of the accuracy of a predictive model consists of comparing which proportion of companies identified as high risk by the model go on to experience an actual ransomware event.[92] An example would be a model that predicts companies that are in the top twenty percent worst risks for experiencing ransomware account for over ninety percent of actual ransomware events.

One challenge with optimal validation is a confluence of lack of incident data, the need to update models in line with changing cyber risk, and the lag time in incorporating reported incidents into the model.[93] As such, other approaches can be assistive. For example, ransomware risks that are segmented based on a risk score/rating can be validated by backtesting—observing whether or not they had such an incident in the twelve months following the rating date—would inspire confidence that the model is performing in line with insurance objectives.[94] Another variation is to use area under the curve ("AUC") to measure how the predictive model performs compared to a baseline model built on revenue and industry, where the higher the positive result indicates the quantitative strength of the lift provided by the predictive model.[95] Even when the model prediction differs greatly from observed outcomes, there is value in identifying any weaknesses and limitations that account for the difference, and iterating the model to learn from the data. Comparing expectations and results for

---

[90] *See* Cooksey*, supra* note 88 ("[E]ven good predictive models can begin to deteriorate over time as the data on which it is based gets older and older. A need exists to track this to know when to update a model.").

[91] *See id.* ("The best way to verify the functioning of a good model and to know when it needs to be refreshed is to monitor that model's business performance.").

[92] Correspondence with Chris Cooksey, Head Actuary, Guidewire Analytics (Jan. 2021).

[93] *See* Roosevelt C. Mosley Jr. & Emily Stoll, PowerPoint Presentation: Process of Developing Predictive Models 10 (NAIC Insurance Summit 2017), https://www.actuary.org/sites/default/files/files/predictive-modeling/NAIC_PM_Section2.pdf.

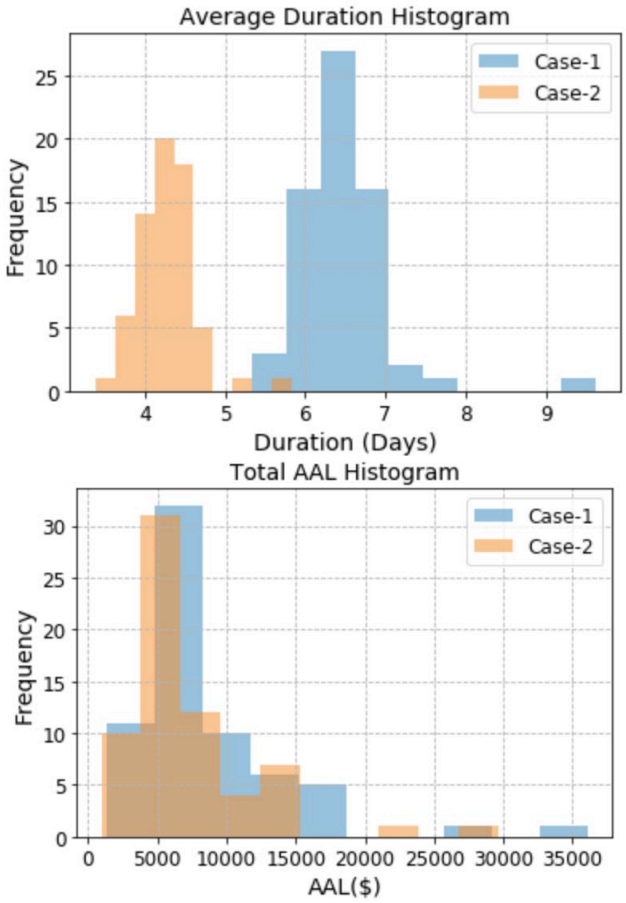
[94] Correspondence with Chris Cooksey, Head Actuary, Guidewire Analytics (Jan. 2021).

[95] *See* Dan Lans, *Illustrating Predictive Models with the ROC Curve*, TOWARDS DATA SCI. (June 30, 2019), https://towardsdatascience.com/illustrating-predictive-models-with-the-roc-curve-67e7b3aa8914.

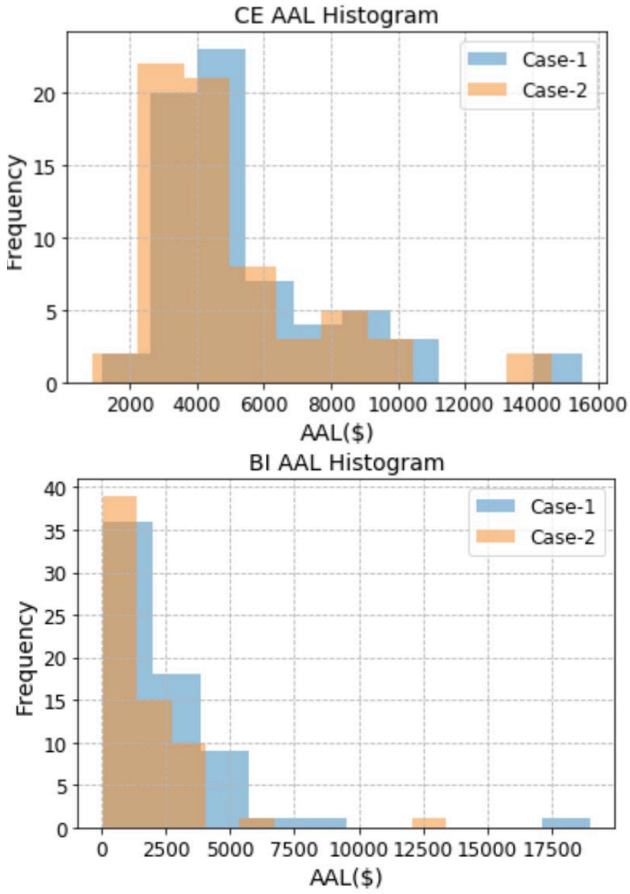
predictive models based on both event data and expert judgment offers myriad adaptation benefits such as: identifying gaps in our understanding of ransomware risk; making assumptions explicit; creating institutional memory; providing a grounded decision support tool; and generating insights.

The difference in model outputs that are informed by ground truth versus generalized or conjectured inputs can be significant. For instance, consider a ransomware loss model that accounts for the probability that ransomware victims have *backup* technology compared to a more nuanced model that has parameters for the probability of *successful restoration* from backup controls. The results illustrated in Figure 5 show the differing outputs of these two models. Specifically, the first incorporates the ground truth that roughly half of companies have backup controls and assumes full restoration (referenced in Figure 5 as Case 2) and the second considers that an average of fifty percent of those restorations will fail (referenced in Figure 5 as Case 1). When assessing predicted severity for this sample portfolio, we see longer business interruption ("BI") duration and larger BI and cyber extortion ("CE") average annual losses ("AALs")—all significant details for cyber underwriting.

Figure 5: Difference in Theoretical v. Empirical Data Informed Model Output[96]



[96] Guidewire Cyence, Cyber Risk Analytics Data (on file with Guidewire Software Inc.).



F. EXTORTION PAYMENT POLICY REFORM

But for cryptocurrency, the selective pressure introduced by ransomware incidents and claims would be unremarkable. Ransomware payments are typically demanded in cryptocurrency in exchange for a digital key to decrypt files and restore victims' access to systems or data.[97]

---

[97] *Insurance Watch: Ransomware*, CIFFA (Dec. 9, 2021), https://ciffa.com/ffo/insurance-watch-ransomware/.

Cryptocurrency has proven to be the *killer app* for ransomware attackers.[98] It optimizes payout efficiency by allowing direct extortion payment from victims rather than having to launder stolen data through the black market, and it lowers attribution risk by providing another layer of pseudonymity[99] to evade law enforcement's track and trace.[100]

Given the pivotal role that cryptocurrency plays in the ransomware ecosystem, governance layer adaptation interventions around extortion payment stands to reason. Options range from targeting supply side by outright prohibition of ransomware pay-outs, to aiming at the demand side by trying to improve attribution and enforcement against bad actors. An open question is if current regulations and policy appropriately guard against facilitating ransomware, or if more robust prohibitions are needed. These efforts include the Office of Foreign Assets Control's ("OFAC") Advisory on the sanction risks of paying ransoms[101] and the Financial Crimes Enforcement Network ("FINCEN") Advisory on reporting ransomware red flag indicators.[102] Softer law signals also emanate from law enforcement guidance that businesses generally should not pay ransoms to decrypt

---

[98] *See* Greg Myre, *How Bitcoin Has Fueled Ransomware Attacks*, NPR (June 10, 2021, 5:06 AM), https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks; DAVID W. PERKINS, CONG. RSCH. SERV., R45427, CRYPTOCURRENCY: THE ECONOMICS OF MONEY AND SELECTED POLICY ISSUES 7–8 (2020).

[99] "Cryptocurrency users typically use a pseudonymous address to identify each other and a passcode or *private key* to make changes to a public ledger in order to transfer value between accounts." PERKINS, *supra* note 98, at i.

[100] *See* Myre, *supra* note 98.

[101] On October 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an advisory to companies providing services to victims of ransomware attacks, informing them of the potential sanctions risks for facilitating ransomware payments to designated persons (individuals or an entity) who conduct certain cyberattacks. U.S. DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [hereinafter TREASURY DEP'T ADVISORY].

[102] U.S. TREASURY FIN. CRIMES ENF'T NETWORK, FIN-2020-A006, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 5–6 (2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

files.[103] In addition, the U.S. Department of Justice ("DOJ") has promulgated a new enforcement framework aimed at individuals that facilitate illicit trade using cryptocurrencies.[104]

The impact of these light touch governance interventions on cyber insurer adaptation to ransomware appears to be inadequate, but it may be too early to tell. The two advisories do not carry the force of law.[105] In fact, the OFAC advisory is not even a new policy or regulation, but a reminder of the existing regulatory framework in effect when paying funds to entities on the Specially Designated Nationals and Blocked Persons ("SDN") list.[106] Up until September 21, 2021, there had been no civil penalties levied against victim companies, insurers, or response firms for paying or facilitating the payment of cyber extortion.[107] There is a fair amount of enforcement discretion, and sanctions nexus decisions turn on attribution, which is rife with uncertainty in most cyberattacks, let alone when trying to identify if crypto wallet owners, or the source of malware are affiliated with an SDN.[108] "In a nutshell, since the ransom is often lower than the cost of recovery, business interruption and lost business – the convergence of which can spell

---

[103] *See* FBI, This Week*, Advocating Against Ransomware Payment Demands*, FED. BUREAU OF INVESTIGATION (Aug. 22, 2019), https://www.fbi.gov/audio-repository/ftw-podcast-ransomware-082219.mp3/view.

[104] Operators of mixers and tumblers "can be criminally liable for money laundering because these mixers and tumblers are designed specifically to 'conceal or disguise the nature, the location, the source, the ownership, or the control' of a financial transaction." U.S DEP'T OF JUST., OFF. OF THE DEPUTY ATT'Y GEN.'S CYBER-DIGITAL TASK FORCE, CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 41–44 (2020), https://www.justice.gov/ag/page/file/1326061/download.

[105] TREASURY DEP'T ADVISORY, *supra* note 101, at 1 n.1; U.S. TREASURY FIN. CRIMES ENF'T NETWORK, *supra* note 102.

[106] *See* TREASURY DEP'T ADVISORY, *supra* note 101, at 3. *See also* Andrew G. Simpson, *Weighing Effects of Treasury's Ransomware Pay Warnings on Cyber Victims and Insurers*, INS. J. (Oct. 15, 2020), https://www.insurancejournal.com/news/national/2020/10/15/586564.htm.

[107] *See* Michael T. Borgia & Dsu-Wei Yuen, *OFAC Makes Waves in Fight Against Ransomware, but Practical Effects Unclear*, DAVIS WRIGHT TREMAINE LLP (Oct. 1, 2021), https://www.dwt.com/blogs/privacy--security-law-blog/2021/10/ofac-updated-ransomware-advisory#print.

[108] *See id.* ("Most payments to ransomware attackers do not have an apparent nexus to OFAC-sanctioned persons, so whether the Updated Advisory will defer many payments is hard to say.").

financial death – many victims and insurers simply pay the ransom and risk sanctions."[109]

As expected, insurers have taken a rational economics approach to ransomware, leading to a growing sentiment that the industry is worsening the problem by paying extortions.[110] While causality has yet to be proven, indicators suggest that ransomware is responsible for increasing Bitcoin prices.[111]

Figure 6: Correlation between the rise in Bitcoin price and ransomware attacks from May 1, 2019, to September 2, 2019[112]

---

[109] Alex Scroxton, *Is it Time to Ban Ransomware Insurance Payments?*, COMPUTERWEEKLY.COM (Feb. 11, 2021), https://www.computerweekly.com/feature/Is-it-time-to-ban-ransomware-insurance-payments (quoting author). *See also* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00 AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks (quoting Fabian Wosar, chief technology officer for anti-virus provider Emsisoft, "[insurance companies] will pay anything, as long as it is cheaper than the loss of revenue they have to cover otherwise.").

[110] *See* Dudley, *supra* note 109.

[111] *See* Jareth, *Is Ransomware Driving Up the Price of Bitcoin?*, EMSISOFT: BLOG (Sept. 3, 2019), https://blog.emsisoft.com/en/33977/is-ransomware-driving-up-the-price-of-bitcoin/. *See also infra* Figure 6.

[112] *Id.*

Insurance adaptation in this context must consider interventions that are appropriate for what needs to be acknowledged as a collective action problem. While on an individual policy level it may be rational to pay extortionists. However, this approach when viewed in the cumulative and long-term, likely encourages ransomers (and arguably other bad actors whose profits stem from crypto market price increases).[113] Combined with the loose legal framework that can discourage payment transparency by victims, we have the high reward/low risk environment that likely predicates terrorist and state-sponsored actor affairs.

Insurers can double-down on DFIR to try and bolster post hoc attribution and enforcement, including trying to clawback payments,[114] or seek a license from OFAC to pay the ransom.[115] These approaches, however, are point solutions to a systemic problem, and thus fall short of what is needed to adapt. Invariably none of these approaches will alter the dynamics that inform the economics of ransomware payment strategy. Investigation and legal process can be protracted relative to business interruption costs, not to mention when life and safety of individuals are at stake in cases involving attacks on hospitals, and attackers can countermove to anonymity enhancing forms of payment.[116]

The other defining aspect of the ransomware risk ecosystem is the simple fact that "weak cybersecurity in affected organisations is the main reason why cybercriminals have been so successful in extorting money from them."[117] By removing incentives for attackers, the knock-on effect will

---

[113] *See* Dudley, *supra* note 109.

[114] *See, e.g.*, AA v. Persons Unknown [2019] EWHC (Comm) 3556, [26]–[27] (explaining how a UK insurer was able to recover ransom payments by tracing a wallet address at an exchange and obtaining an asset preservation order to disclose information on the individuals holding the accounts to which the payment had been transferred).

[115] TREASURY DEP'T ADVISORY, *supra* note 101, at 4.

[116] For examples of anonymity enhancing forms of payment see MONERO, https://www.getmonero.org/resources/about/ (last visited Mar. 2, 2022); ZCASH, https://z.cash/support/faq/ (last visited Mar. 2, 2022); DASH, https://www.dash.org/faq/ (last visited Mar. 2, 2022).

[117] Lena Connolly & David S. Wall, *Hackers are Making Personalised Ransomware to Target the Most Profitable and Vulnerable,* CONVERSATION (Mar. 15, 2019, 10:54 AM), https://theconversation.com/hackers-are-making-personalised-ransomware-to-target-the-most-profitable-and-vulnerable-113583.

serve as a further incentive for companies to address the fundamental blocking and tackling discussed prior and thus diminish the very preconditions for ransomware to succeed. The adaptation is a "whole-of-insurance, self-regulatory approach that establishes a ransom non-payment policy."[118] This is already being embraced on the victim-payer side[119] and certainly is not without precedent on the carrier end.[120] And it may be possible "by leveraging traditional compliance clause provisions, such as excluding payments that are subject to existing regulatory restrictions or freezing policy benefits subject to government oversight of sanctions violations compliance."[121] Alternatively, "the industry can act on its own and take a policy stance to refuse payment, barring defined, exceptional circumstances that threaten life and safety."[122]

V. SOLUTIONS HIDING IN PLAIN SIGHT

Hackers have the upper hand, in large part because they have adapted, forming partnerships and Ransomware as a Service ("RaaS") business models, constantly improving their malware, and operationalizing their motive, means, and opportunity more effectively.[123] "[T]he underground ransomware economy is now an industry that resemble commercial software – complete with development, support, distribution,

---

See also ALLIANZ GLOBAL CORPORATE & SPECIALTY, RANSOMWARE TRENDS: RISK AND RESILIENCE 17 (2021), https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/agcs-ransomware-trends-risks-and-resilience.pdf ("Hackers will typically hit those businesses with the weakest defenses first . . . .").

[118] Scroxton, *supra* note 109 (quoting author).

[119] United States Conference of Mayors, Opposing Payment to Ransomware Attack Perpetrators, 87th Annual Meeting, Resolution Adopted 2019, https://www.usmayors.org/the-conference/resolutions/?category=a0D4N00000FCb3LUAT&meeting=87th%20Annual%20Meeting (highlighting that more than 225 US mayors signed on to a resolution not to pay ransoms to hackers).

[120] *See, e.g.*, Matt Sheehan, *New Lloyd's Mandate to Require Clarity on Silent Cyber Coverage*, REINSURANCE NEWS (July 4, 2019), https://www.reinsurancene.ws/new-lloyds-mandate-to-require-clarity-on-silent-cyber-coverage/.

[121] Scroxton, *supra* note 109 (quoting author).

[122] Scroxton, *supra* note 109 (quoting author).

[123] *See* ALLIANZ GLOBAL CORPORATE & SPECIALTY, *supra* note 117, at 4; *The Ransomware Business Model That You're Probably Not Prepared for*, CYBERTALK.ORG (Aug. 14, 2020), https://www.cybertalk.org/2020/08/14/the-ransomware-business-model-that-youre-probably-not-prepared-for/.

quality assurance and even help desks."[124] The same cannot be said about the cyber insurance industry when it comes to ransomware peril coverage.

Critics contend that the cyber risk underwriting challenges lack foundational support to reduce cyber exposure.[125] While these arguments are well-founded, the proposed adaptation framework herein is aimed at addressing those capability gaps. To be sure, there are clear signals that these adaptations are taking root. There is more scrutiny of organizations' InfoSec controls for ransomware in the underwriting process pre-incidents.[126] Some insurers are also committing to proactive risk management coordination, security training, and network security vulnerability testing.[127] The notion of going beyond indemnifying, pooling, and diversifying risks to actively managing the cyber risk is not novel—it is what insurers of data breach instituted in the wake of breach notification regulation and privacy law compliance.[128] So the groundwork has been laid for embracing security best practices, cyber risk assessments and health checks, third party digital forensics and incident response vendors, evolving policy language, and risk management services. The difference with ransomware is there is no legal compliance driver upon which to rely, so simply transplanting a breach

---

[124] CARBON BLACK, THE RANSOMWARE ECONOMY 7 (2017).

[125] *See* CISA REPORT, *supra* note 82, at 15–16.

[126] *See* MARSH, MARKETS: PRICING INCREASES MODERATE IN SECOND QUARTER 6, 10 (2021), https://www.marsh.com/us/services/international-placement-services/insights/global-insurance-market-index-q2-2021.html; ALLIANZ GLOBAL CORPORATE & SPECIALTY, *supra* note 117, at 15; Michael Hill, *Buying Cyber Insurance in 2021? Expect Greater Scrutiny, Higher Premiums*, CSO (Apr. 27, 2021, 2:00 AM), https://www.csoonline.com/article/3616595/buying-cyber-insurance-in-2021-expect-greater-scrutiny-higher-premiums-thanks-to-ransomware-supply.html.

[127] *See, e.g.*, *Loss Mitigation for Cyber Policyholders*, CHUBB: CYBER SERVICES, https://www.chubb.com/us-en/business-insurance/loss-mitigation-for-cyber-policyholders.html (last visited Mar. 6, 2022); AM. INT'L GRP., INC., CYBER LOSS CONTROL SERVICES (2021), https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-loss-control-services-all.pdf; *Risk Management Tools & Resources*, BEAZLEY GRP., https://www.beazley.com/united_kingdom/cyber_and_tech/beazley_breach_response/cyber_services/risk_management_tools_and_resources.html (last visited Mar. 6, 2022).

[128] *See, e.g.*, Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 LAW & SOC. INQUIRY 417 (2018).

compliance strategy will not work. The industry must be a forcing function onto itself.

Is the cyber insurance industry at an inflection point due to ransomware? That answer is always hard to know while steeped in the middle of it. Just like the human appendix, some characteristics of the insurance culture, governance and infrastructure may be outdated adaptations, still hanging on past the point of their usefulness. The culture, governance and infrastructure layers require a change in both disposition and focus; along with an expanded notion of what opportunity means. Opportunity comprises more than just altering premiums and limits to meet acceptable loss ratios for the industry while underserving risk transfer needs in the market. Too narrow an understanding of opportunity has led to policies and practices that have rendered cyber insurance impotent to addressing on the ground ransomware cyber risk. The innovation that will ensure resiliency and impact ransomware risk itself is the opportunity that a Darwinian approach promises to deliver.

"COMMONLY ACCEPTED NOTIONS OF INSURANCE" FOR CAPTIVES IN TAX CASES ARE NOT COMMON NOTIONS OF INSURANCE IN THE INSURANCE INDUSTRY

HAROLD WESTON*

TABLE OF CONTENTS

INTRODUCTION

Experts in insurance have a hard time defining insurance. The insurance field allows multiple definitions to co-exist in a pragmatic and highly-regulated marketplace. It is an ecosystem of regulations, law, theory, probabilistic mathematics, and economics. The tax courts, deciding tax deduction questions involving premiums paid to captive insurance companies, have settled on their own definition of insurance, which they call

* Clinical Associate Professor of Risk Management and Insurance, Georgia State University, Robinson College of Business, and College of Law (secondary appointment), Atlanta, Georgia.

"commonly accepted notions of insurance."[1] These notions are far removed from the criteria (or notions) known to the insurance domain. In fact, most of the tax notions of insurance are neither common nor even relevant to what insurance is. An incorrect understanding of insurance could be a problem for how the tax courts decide whether the premiums paid to captive insurers are appropriate and deductible business expenses. This article reviews the tax decisions that have led to the mistaken, and in fact not, "commonly accepted notions of insurance." It reviews the history, development, practice, and regulation of insurance to show that a licensed, regulated insurance company can lawfully do far more than what the tax court decisions believe, regardless of whether the insurer is a standard-type corporate insurance company, mutual insurer, surplus lines insurer, or captive insurer. This paper also examines the risk distribution concept and concludes that the great variety in how insurance is actually done as a business shows that risk distribution, as the tax courts use the concept, is sometimes unreliable as a guide to determine the practice of insurance.

I. WHY CAPTIVE INSURANCE COMPANIES ARE A PROBLEM FOR THE IRS

Captive insurers are regulated insurance companies, like any other insurance company, except they are owned by a parent corporation to insure the parent corporation's insurable risks, rather than the insurable risks of individuals and firms outside the corporation.[2] The reasons a corporate parent might form a captive insurance company include "excessive pricing, limited capacity, risks that are uninsurable in the 'traditional' insurance market, or the desire for a more cost-efficient risk financing mechanism."[3] A standard treatise on captive insurance states, "[c]aptive insurance is utilized by insureds that choose to put their own capital at risk by creating

---

[1] The phrase appears in several tax court cases. *See, e.g.*, AMERCO & Subsidiaries v. Comm'r, 96 T.C. 18, 42 (1991), *aff'd sub nom.* AMERCO, Inc. v. Comm'r, 979 F.2d 162 (9th Cir. 1992); Harper Grp. & Includible Subsidiaries v. Comm'r, 96 T.C. 45, 60 (1991), *aff'd*, 979 F.2d 1341 (9th Cir. 1992); Rent-A-Ctr., Inc. v. Comm'r, 142 T.C. 1, 13 (2014); Avrahami v. Comm'r, 149 T.C. 144, 181 (2017).

[2] William Byrnes, *Captive Insurance Arrangements, in* 2 NEW APPLEMAN ON INSURANCE LAW § 12.16[1] (Jeffrey E. Thomas & Martin F. Grace eds., Library ed., LEXIS, database updated May 2021).

[3] Stephen T. Bird, *Reasons for Forming a Captive*, INT'L RISK MGMT. INST.: RISK FIN., https://www.irmi.com/online/rf/ch004/1l04h000/al04h001-reasons-for-forming-a-captive.aspx (last visited Jan. 19, 2022).

their own insurance company, or utilizing an existing special purpose insurer, working outside of the commercial insurance marketplace to achieve their risk financing objectives."[4] Teasing this apart shows the following elements are required: (1) that the insured is "willing and able to contribute risk capital;"[5] (2) that the insurer is "working outside of the commercial insurance marketplace"[6] by being owned and controlled by the insured, but is distinguishable from the mutual insurance company where there are many owners with no control; and (3) that the captive is "to achieve their [insured owner's] risk financing objectives."[7] A pure captive insurer is one that writes the risks of the insured, which may include "an unrelated risk to satisfy the risk financing objectives of the owner."[8] Control over the risk financing is fundamental to captives.

> Inevitably, insureds wishing to improve control over the way that insurance is used to finance their risks seek to increase their control over the insurer. This explains why the second essential element of captive insurance is that it involves financing risks using special purpose insurers, companies that operate or provide programs outside of the traditionally regulated commercial marketplace.[9]

Another treatise on captive insurance explains, "[c]aptive insurance is the zenith of risk financing. Captives provide businesses the ultimate flexibility regarding coverage, claims, premium, and control, while further offering a bevy of valuable attributes such as lucrative dividends and innovative financing techniques . . . ."[10]

Setting up, funding, managing, and operating a captive insurer is a complex operation. It is suitable only after a "feasibility study" shows a captive is sensible and management determines it has the capability to run a

---

[4] KATHRYN A. WESTOVER, CAPTIVES AND THE MANAGEMENT OF RISK 5 (2nd ed. 2006).

[5] *Id.* at 6.

[6] *Id.*

[7] *Id.* at 7.

[8] *Id.* at 8. Furthermore, such distinction of unrelated risk has some relevance later to challenges by the Internal Revenue Service to captive insurers and the spread of risk. *See infra* Part III.

[9] WESTOVER, *supra* note 4, at 7.

[10] MATTHEW QUEEN & LIGHT TOWNSEND, MODERN CAPTIVE INSURANCE: A LEGAL GUIDE TO FORMATION, OPERATION, AND EXIT STRATEGIES xxi-xxii (2019).

captive insurer (with appropriate managers).[11] There must be financial advantages, such as possible tax advantages, for a business to go through the expense and trouble of using a captive insurer.[12] However, that analysis, and the particulars of the tax aspects, are not relevant to this paper.

The Internal Revenue Service ("IRS") has long challenged the tax deductions made by corporations, big and small, when they deduct the premiums paid to their captive insurance companies.[13] There have been good reasons in some situations for doubting the deductible expenses of insurance premiums paid to captive insurers based on the economic-substance doctrine, which is used to evaluate the transaction.[14] Yet the IRS has often challenged the deductions based on its ideas of what constitutes insurance and what constitutes an insurance company.[15] This is a different problem because captive insurers are established and regulated by state insurance commissioners or off-shore insurance regulators—wherever the parent corporation chooses to set up its captive insurer.[16]

---

[11] *See* Stephen T. Bird, *Captive Feasibility Study*, INT'L RISK MGMT. INST.: RISK FIN., https://www.irmi.com/online/rf/ch004/1l04h000/captive-feasibility/bl04h060a-feasibility-studies.aspx (last visited Jan. 19, 2022).

[12] *See* Byrnes, *supra* note 2 ("While the tax benefits of captive insurance are often not the primary motivator for using a captive insurance structure, they can provide motivation for forming a captive instead of using commercial insurance.").

[13] *See generally* Li-Ming Han & Gene C. Lai, *The Tax Deductibility of Premiums Paid to Captive Insurers: A Risk Reduction Approach*, 58 J. RISK & INS. 47 (1991); Philip Garrett Panitz, *Captive Insurance: Avoiding the Risks*, J. OF ACCT. (June 1, 2018), https://www.journalofaccountancy.com/issues/2018/jun/captive-insurance-entities.html.

[14] Salty Brine I, Ltd. v. United States, No. 5:10-CV-108-C, 2013 U.S. Dist. LEXIS 98509, at *43 (N.D. Tex. May 16, 2013); Klamath Strategic Inv. Fund v. United States, 568 F.3d 537, 545 (5th Cir. 2009); Frank Lyon Co. v. United States, 435 U.S. 561, 583–84, (1978).

[15] *See generally* Han & Lai, *supra* note 13; Panitz, *supra* note 13.

[16] *See* McCarran-Ferguson Act, 15 U.S.C. §§ 1011–1015. *See also* WESTOVER, *supra* note 4, at 146–47; QUEEN & TOWNSEND, *supra* note 10, at 156–57; Gary M. Cohen, *History of Insurance Regulation, in* 2 NEW APPLEMAN ON INSURANCE LAW § 8.01 (Jeffrey E. Thomas & Martin F. Grace eds., Library ed. 2021). Illustrative statutes of some of the leading state domiciles for captive insurers include VT. STAT. ANN. tit. 8, § 6001(5) (LEXIS through 2021 Adj. Sess.) ("'Captive insurance company' means any pure captive insurance company, association captive insurance company, sponsored captive insurance company, industrial insured captive insurance company, agency captive insurance company, risk retention group, affiliated reinsurance company, or special purpose financial insurance company

The IRS has several criteria to decide whether the captive insurer sufficiently resembles a proper insurance company—where premiums paid to the captive resemble premiums paid to any insurer in order to be deductible as an ordinary business expense. The criteria are: (1) an insurable risk to transfer; (2) risk-shifting; (3) risk-distribution; and (4) insurance "in its commonly accepted sense,"[17] sometimes called "common notions of insurance."[18]

Risk shifting is usually easy enough to find—unless the risk circles back to the parent in a "circular flow of funds."[19] Risk distribution is easy to find when there are a large number of insurable exposures, such as office properties or a fleet of vehicles, but is harder to find for small businesses with few properties or for liability. Also, questions about vertical distribution may exist when reinsurance is used.[20] An examination of how risk distribution actually exists, historically and currently, shows that this is sometimes a difficult concept to properly observe.

"Commonly accepted notions of insurance" sounds sensible, except such notions are limited to the tax cases, not the insurance cases. In fact, the tax case notions are non-existent in the insurance statutes, insurance cases, and the practices of insurance.[21] Moreover, old and new treatises of insurance show a completely different view of the practices of insurance than what the IRS and the tax courts view as insurance.[22]

II. ORIGINS OF THE TAX COURT CRITERIA FOR EVALUATING INSURANCE

The first mention of "commonly accepted notions of insurance" appeared in *Helvering v. Le Gierse*.[23] The case involved a life insurance

---

formed or licensed under the provisions of this chapter." (footnote omitted)); COLO. REV. STAT. ANN. § 10-6-103 (LEXIS through 2022 Reg. Sess.); S.C. CODE ANN. § 38-90-10 (LEXIS through 2022 Reg. Sess.); TENN. CODE ANN. § 56-13-101 (LEXIS through 2022 Re. Sess.).

[17] AMERCO & Subsidiaries v. Comm'r, 96 T.C. 18, 38 (1991).

[18] Avrahami v. Comm'r, 149 T.C. 144, 180 (2017).

[19] *See id.* at 185; Rent-A-Ctr., Inc. v. Comm'r, 142 T.C. 1, 11–12 (2014).

[20] *See* 1 GRAYDON S. STARING & DEAN HANSELL, LAW OF REINSURANCE § 1:1 (2022 ed., Westlaw, database updated Mar. 2022) ("Usually only a part of a loss or liability is reinsured. Sometimes, however, it may be the entire loss or liability."). *See also id.* § 1:3 (discussing horizontal and vertical risk distribution).

[21] *See* discussion *infra* Part IV.B.

[22] *See* discussion *infra* Part IV.A.

[23] Helvering v. Le Gierse, 312 U.S. 531 (1941).

company that sold to the taxpayer an unusual combination of an annuity contract and a life insurance policy.[24] The purpose of the policy was, evidently, to generate an annuity payment from the life insurance and then have the unpaid premiums move via life insurance to a beneficiary, and, crucially, avoid that value being included in the gross estate and subject to estate tax.[25] Life insurance has long been used for this precise purpose—to avoid the estate tax and use a life insurance trust to hold the insurance—so long as the purchase is made at least three years in advance.[26] The generation of an annuity payment was a clever idea to allow the decedent to have an income from money that otherwise would be valued in the estate if the insurance proceeds exceeded $40,000 (then the exclusion amount for the estate tax).[27] The Supreme Court found a scant definition of insurance in the tax regulations, and thus, sought alternate definitions.[28] It found that "courts and commentators" agreed that "risk-shifting and risk-distributing are essential to a life insurance contract."[29] Life insurance met those requirements, and thus, it was "'insurance' in its commonly accepted sense."[30] This was all the Supreme Court said about what stands for insurance in the commonly accepted sense. In the particular facts of the case, the Supreme Court found that the combination of the annuity and life

---

[24] *Id.* at 536–37.

[25] *Id.*

[26] *See* 3 J. MARTIN BURKE, MICHAEL K. FRIEL, & ELAINE HIGHTOWER GAGLIARDI, MODERN ESTATE PLANNING § 39.10 (2nd ed., LEXIS, database updated May 2022). *See also* 26 U.S.C. § 2042.

[27] *See Helvering*, 312 U.S. at 537–38:

> Section 302 of the Revenue Act of 1926 . . . provides: 'The value of the gross estate of the decedent shall be determined by including the value at the time of his death of all property, real or personal, tangible or intangible . . . (g) To the extent of the amount receivable by the executor as insurance under policies taken out by the decedent upon his own life; and to the extent of the excess over $40,000 of the amount receivable by all other beneficiaries as insurance under policies taken out by the decedent upon his own life.' Thus the basic question is whether the amounts received here are amounts 'receivable as insurance' within the meaning of s[ection] 302(g).

[28] *Id.* at 538.

[29] *Id.* at 539.

[30] *Id.* at 540. The Supreme Court later said the same thing in *Grp. Life & Health Ins. Co. v. Royal Drug Co.*, 440 U.S. 205, 211 (1979), citing to standard insurance treatises but not citing to *Helvering*.

insurance contracts, though separate, "counteracted each other. . . . The fact remains that annuity and insurance are opposites; in this combination the one neutralizes the risk customarily inherent in the other. From the company's viewpoint, insurance looks to longevity, annuity to transiency."[31] The Supreme Court explained:

> Here the total consideration was prepaid and exceeded the face value of the "insurance" policy. The excess financed loading and other incidental charges. Any risk that the prepayment would earn less than the amount paid to respondent as an annuity was an investment risk similar to the risk assumed by a bank; it was not an insurance risk as explained above. It follows that the sums payable to a specific beneficiary here are not within the scope of s[ection] 302(g). The only remaining question is whether they are taxable.[32]

The next case also involved a death payment, but there was no life insurer involved to pay the proceeds upon death. In *All v. McCobb*, an executive of the Standard Oil Company of New Jersey received a "'retirement allowance' under an 'Annuity Plan for the Employees of Standard Oil Company (New Jersey) and its Participating Subsidiaries Effective January 1, 1932'"[33] and the employer also provided a death benefit plan for the executives that paid twelve equal payments to the survivor upon the death of the executive.[34] An executive died, the survivor received the extra payments, and the survivor sought to exclude them from the decedent's estate as life insurance proceeds.[35] The IRS contested the exclusion.[36] The Supreme Court agreed with the commissioner that because there was no insurance involved and no premium was paid, the proceeds did not exceed any premium (of which there was none), and these were extra payments made by the employer.[37]

> The decedent in no way shifted to the company the risk that his death would come prematurely and before the company,

---

[31] *Helvering,* 312 U.S. at 541.
[32] *Id.* at 542.
[33] All v. McCobb, 321 F.2d 633, 634 (2d Cir. 1963).
[34] *Id.*
[35] *Id.* at 635.
[36] *Id.*
[37] *Id.* at 637.

> as insurer, had received premiums by or on his account in a sum equal to the amount required to be paid to the beneficiary. The company in no way gambled with the decedent that he would live a long life and that it would recover by periodic assessments before his death the amount to be paid to the beneficiary. It made no difference to the company, so far as any fund was concerned, whether the decedent died prematurely or not.[38]

Later cases citing to *Le Gierse* also considered the estate tax.[39]

The tax court inquiry into what is insurance changed from life insurance to bail bonds in *Allied Fidelity Corp. v. Commissioner*.[40] The court considered whether a bail bond company was an insurance company for purposes of whether to classify its expenses and reserves as deductible or excludable expenses.[41] The problem was whether bail bonds were close enough to surety bonds, because surety is a type of insurance. This raised the question of what insurance was. The court stated it lacked any place to look for that definition of insurance for tax purposes, and even outside of the tax law there were varied definitions.[42]

> We are provided with no helpful, freestanding definitions of the terms 'insurance' and 'insurance company' for Federal tax purposes. It is clear that our decision is not controlled by nontax classifications and that characterization of particular corporations depends not on labels or certificated powers but on the character of the business actually conducted and that, in the absence of other guides, we should presume Congress to have used words in their ordinary and commonly understood sense. . . .

---

[38] *Id.*

[39] *See, e.g.*, Proutt's Est. v. Comm'r, 125 F.2d 591 (6th Cir. 1942) (life insurance); United States v. First Nat'l Bank & Trust Co. of Minneapolis, 133 F.2d 886 (8th Cir. 1943) (life insurance); Cary v. United States, 141 F. Supp. 750 (D. Neb. 1956) (health insurance); Edgar v. Comm'r, 39 T.C.M (CCH) 816 (1979) (life insurance); *In re* Newton's Estate, 32 N.Y.S.2d 473 (N.Y Sur. Ct. 1941) (life insurance).

[40] Allied Fid. Corp. v. Comm'r, 66 T.C. 1068 (1976), *aff'd*, 572 F.2d 1190 (7th Cir. 1978).

[41] *Id.*

[42] *Id.* at 1073.

> In resolving this issue, we are unable to ascribe much significance to the fact that AFIC's bail bonding business was subject to regulation under the insurance laws of the various States in which it did business. Such regulation amounts to no more than a recognition that a corporate bail bondsman is ordinarily an insurance or surety company, not that bail bonding is insurance. . . .
>
> In common understanding, an insurance contract is an agreement to protect the insured (or a third-party beneficiary) against a direct or indirect economic loss arising from a defined contingency. . . . By contrast, the principal obligation of the bail surety at common law was to produce the defendant at trial, an obligation for which the monetary bond was merely an assurance of, or inducement to, performance.[43]

The court concluded that bail bonds were not insurance, even though bail bond companies were regulated as insurers.[44] This is because:

> The focus of the bail system remains on balancing the accused's interest in personal liberty against the giving of adequate assurance of his presence during the criminal proceedings not on protecting the Government against economic loss. Thus, the surety is still regarded as contracting principally to assume the Government's duty of supervising the defendant, rather than to compensate it for an economic loss.[45]

Later tax opinions upheld this ruling but recognized that surety companies are insurance.[46]

It is from these tax cases, usually involving life insurance as noted earlier, that the IRS and the tax courts made the leap to what is insurance for property and liability exposures and what constitutes insurance for a property and casualty insurer. This is a big leap, and it does not land well.

---

[43] *Id.* at 1073–74 (citations omitted).

[44] *Id.* at 1076.

[45] *Id.* at 1075 (citation omitted).

[46] *See* I.R.S. Gen. Couns. Mem. 39,154 (Mar. 1, 1984); I.R.S. Tech. Adv. Mem. 84-06-001 (Mar. 11, 1983).

III. THE CAPTIVE INSURANCE CASES' USE OF "COMMONLY ACCEPTED NOTIONS" TO DETERMINE INSURANCE

The expansion in the use of captive insurance companies in the 1990's led to some questionable uses of tax deductions by the parent corporations.[47] The IRS challenged these and were sometimes successful. Part of the challenge was to determine whether these captive insurance companies really were operating as an insurer for the parent corporation. The IRS and the tax courts then examined whether the captives were actually doing insurance—despite the fact that insurance regulatory bodies onshore and offshore had licensed, allowed, supervised and regulated these companies to operate as insurance companies. The IRS and the tax courts disregarded the de facto insurance license and regulatory approval, and instead looked back at earlier court decisions that tried to define insurance. Remember, those earlier decisions were primarily in the life insurance context and mostly dealt with gross estate value determinations for estate taxes. As will be shown below, this led to some questionable tax case law in the property and casualty sector where many captive companies operate[48]—decisions that are contrary to actual insurance law and practices.

AMERCO v. Commissioner was the first of the captive insurance cases that sought to create its own interpretation of insurance. The court acknowledged that *Le Gierse* was the wrong place for a definition of insurance.[49]

> We begin our discussion with the genesis of the law in this area, *Helvering v. LeGierse*, 312 U.S. 531 (1941). It must be noted that LeGierse was not a captive insurance case; it rather construed and applied the phrase "receivable as insurance" within the meaning of section 302(g) of the Revenue Act of 1926, an estate tax exclusion for life insurance proceeds. Its insights are important, however, because it addressed a statutory void which persists today: the lack of any statutory definition of the term "insurance."

---

[47] In some cases, the tax opportunities drove the use of the captives rather than the feasibility of captives.

[48] Captives can and do operate in other insurance sectors, providing coverage for employee benefit plans, medical stop-loss programs, and some unusual coverages that are not easily slotted within property and casualty insurance.

[49] AMERCO & Subsidiaries v. Comm'r, 96 T.C. 18, 37–38 (1991).

> . . . .
>
> Three basic points are made above: (1) that an insurance transaction must involve "insurance risk;" (2) that insurance involves risk-shifting and risk-distributing; and (3) that, in the absence of a statutory definition, "insurance" is to be defined in its commonly accepted sense. We supplement these insights with another tenet, basic to all our decisions: that matters of Federal income taxation must be resolved with principles of Federal income taxation borne in mind.
>
> These four principles do not yield a definition of insurance. They do, however, create what we believe is the proper framework to be adopted when addressing a question of the existence of insurance for Federal tax purposes. They are not independent or exclusive. Instead, we read them as informing each other and, to the extent not fully consistent, confining each other's potential excesses.[50]

The court then acknowledged that while the states regulate insurance and that the insurer in this case was licensed by that state, that was not "dispositive."[51] *AMERCO* was the fount for the rest of the captive cases.

Harper Group v. Commissioner was another case involving a business that had a property and casualty insurance subsidiary licensed and

---

[50] *Id.* (citations omitted).

[51] *Id.* at 42. The Court also stated:

> We think that the technical indicia of insurance discussed above, supplemented by our analysis of the substance of the transactions at issue, combine to create insurance in the commonly accepted sense. Under this rubric we emphasize the state regulators' definitions of Republic Western as a fully licensed property and casualty insurer, and of the transactions at issue as insurance. While these definitions are not dispositive of the issue before us, they do inform our decision. We note that Congress has delegated to the states the exclusive authority (subject to exception) to regulate the business of insurance.

Id. (citing McCarran-Ferguson Act, 59 Stat. 33 (1945) (codified as amended at 15 U.S.C. §§ 1011–1015)). *See also In re* Stewart's Shops Corp., DTA No. 825745, 2016 WL 1086062, at *21 (N.Y. Div. Tax. App. Mar. 10, 2016).

regulated, however this one in Hong Kong.[52] Again, the court recognized that the company was conducting insurance sufficient for the tax deduction of the corporate parent's premium.[53] *Harper* seems to have created the factors used to determine what is "insurance in its commonly accepted sense" (as contemplated by the tax courts).

> Rampart was both organized and operated as an insurance company. It was regulated by the Insurance Registry of Hong Kong. The adequacy of Rampart's capitalization is not in dispute. The premiums charged by Rampart to its affiliates, as well as to its shippers, were the result of arm's-length transactions. The policies issued by Rampart were valid and binding. In sum, such policies were insurance policies, and the arrangements between the Harper domestic subsidiaries and Rampart constituted insurance, in the commonly accepted sense.[54]

The insured in *Sears, Roebuck & Co. v. Commissioner* sought to deduct loss reserves on mortgage insurance. [55] The related corporate insurer was a subsidiary of the well-known insurer, Allstate Insurance Company, then itself a subsidiary of Sears.[56]

> Allstate is a substantial underwriter, collecting more than $5 billion in premiums annually and possessing more than $2 billion in capital surplus. During the years at issue, Allstate charged Sears approximately $14 million per year for several kinds of insurance. Some 99.75% of Allstate's

---

[52] Harper Grp. & Includible Subsidiaries v. Comm'r, 96 T.C. 45, 47–48 (1991), *aff'd*, 979 F.2d 1341 (9th Cir. 1992).

[53] *Id.* at 60.

[54] *Id.*

[55] Sears, Roebuck & Co. v. Comm'r, 972 F.2d 858, 859–60 (7th Cir. 1992). Of note, this case was different from most of the other captive cases that involved deductibility of premiums paid by the parent.

[56] *Id.*

> premiums came from customers other than Sears, which places 10% to 15% of its insurance with Allstate.[57]

As to the meaning of insurance, the court discounted the applicability of the *Le Gierse* definition.

> What is "insurance" for tax purposes? The Code lacks a definition. *Le Gierse* mentions the combination of risk shifting and risk distribution, but it is a blunder to treat a phrase in an opinion as if it were statutory language. The Court was not writing a definition for all seasons and had no reason to, as the holding of *Le Gierse* is only that paying the "underwriter" more than it promises to return in the event of a casualty is not insurance by any standard.[58]

In fact, "[t]he experts who labored during this trial to define 'insurance' all would have agreed that this dispute is an artifact of the

---

[57] *Id.* at 860. Some useful history of why this tax challenge evolved is stated in the opinion.

> Allstate, founded in 1931, has been selling insurance to Sears since 1945. Everyone, including the Commissioner, has taken Allstate as the prototypical non-captive insurance subsidiary. Until 1977 the Internal Revenue Service respected transactions between non-captive insurers and their parents. In that year the Commissioner decided that a wholly owned subsidiary cannot "insure" its parent's operations, even if the subsidiary's policies are identical in terms and price to those available from third parties. Examples given in this revenue ruling all dealt with captives that had no customers outside the corporate family. After issuing the ruling the Service continued to believe that subsidiaries engaged in "solicitation and acceptance of substantial outside risks" could provide insurance to their parents. But in 1984 the General Counsel reversed course and the Commissioner later announced that all wholly owned insurance subsidiaries should be treated alike. Our task is to decide whether this is correct. We therefore disregard details, which may be found in the Tax Court's opinion. Like the Commissioner, we deem immaterial the nature of the risks Allstate accepted, the terms the parties negotiated, and the precise deductions taken.

Id. at 860–61 (citations omitted).

[58] *Id.* at 861 (citations omitted).

corporate income tax, which by divorcing taxation from real persons' wealth, income, or consumption is bound to combine tricky definitional problems with odd incentives."[59]

The court in *Securitas Holdings, Inc. v. Commissioner* took the *Harper* list and created formal factors to determine "insurance in the commonly accepted sense": "(1) the insurer was organized, operated, and regulated as an insurance company; (2) the insurer was adequately capitalized; (3) the insurance policies were valid and binding; (4) the premiums were reasonable; and (5) the premiums were paid and the losses were satisfied."[60]

Rent-A-Center, Inc. v. Commissioner involved workers' compensation, automobile, and general liability insurance, for thousands of stores and approximately 20,000 employees and 8,000 vehicles.[61] The court cited to the *Harper* factors but decided the case on the obvious risk distribution of all these thousands of insurable exposures.[62]

Avrahami v. Commissioner was a little different because it was a section 831(b) captive that had several signs of concern about how and whether its insurance captive was actually performing insurance.[63] The commonly accepted factors the court used were:

> [W]hether the company was organized, operated, and regulated as an insurance company; whether the insurer was adequately capitalized; whether the policies were valid and binding; whether the premiums were reasonable and the result of an arm's-length transaction; and whether claims were paid. We have also looked at whether the policies covered typical insurance risks and whether there was a legitimate business reason for acquiring insurance from the captive.[64]

Reserve Mechanical Corp. v. Commissioner was also a section 831(b) captive that provided excess insurance over multiple commercially purchased insurance policies and non-standard property policies such as loss of a major customer, weather-related business interruption, tax liability, etc.,

---

[59] *Id.* at 864.

[60] Securitas Holdings, Inc. v. Comm'r, 108 T.C.M. (CCH) 490, 2014 T.C.M. (RIA) ¶ 2014-225, slip op. at 27 (2014).

[61] Rent-A-Ctr. v. Comm'r, 142 T.C. 1, 24 (2014).

[62] *Id.* at 13.

[63] Avrahami v. Comm'r, 149 T.C. 144 (2017).

[64] *Id.* at 191 (citations omitted).

all for a $448,127 premium in 2009.[65] It again formalized the factors to determine insurance in the "commonly accepted sense."[66]

> (1) [W]hether it was created for legitimate nontax reasons;
> (2) whether there was a circular flow of funds;
> (3) whether the entity faced actual and insurable risk;
> (4) whether the policies were arm's-length contracts;
> (5) whether the entity charged actuarially determined premiums;
> (6) whether comparable coverage was more expensive or even available;
> (7) whether it was subject to regulatory control and met minimum statutory requirements;
> (8) whether it was adequately capitalized; and
> (9) whether it paid claims from a separately maintained account.[67]

The court in *Syzygy Insurance Co. v. Commissioner* restated its own factors, mostly based on the non-captive case *R.V.I. Guaranty Co. & Subsidiaries v. Commissioner*,[68] but harking back to the *Harper* case: "(1) whether the company was organized, operated, and regulated as an insurance company; (2) whether it was adequately capitalized; (3) whether the policies were valid and binding; (4) whether premiums were reasonable and the result of arm's-length transactions; and (5) whether claims were paid."[69]

Other cases that deal with this question of "commonly accepted notions of insurance are *Kidde Industries, Inc. v. United States*[70] and *Malone*

---

[65] Rsrv. Mech. Corp. v. Comm'r, 115 T.C.M. (CCH) 1475, 2018 T.C.M. (RIA) ¶ 2018-086, slip op. at 18 (2018), *appeal docketed*, No. 18-9011 (10th Cir. Dec. 27, 2018).

[66] *See id.* at 48–49.

[67] *Id.* at 38–39.

[68] R.V.I. Guar. Co. & Subsidiaries v. Comm'r, 145 T.C. 209 (2015). *See infra* text accompanying notes 73–75.

[69] Syzygy Ins. Co. v. Comm'r, 117 T.C.M. (CCH) 1165, 2019 T.C.M. (RIA) ¶ 2019-034, slip op. at 37 (2019).

[70] Kiddie Indus., Inc. v. United States, 40 Fed. Cl. 42, 51 (Fed. Cl. 1997), *dismissed*, 194 F.3d 1330 (Fed. Cir. 1999).

& Hyde, Inc. v. Commissioner.[71] Several state court tax cases involving captives also used the commonly accepted notions criteria.[72]

The aforementioned non-captive case, *R.V.I.*, took the *Harper* factors, and then (unusually) looked at various state definitions of insurance (including Pennsylvania, Arizona, New York, and Washington) to decide

---

[71] Malone & Hyde, Inc. v. Comm'r, 62 F.3d 835, 839 (6th Cir. 1995).

[72] *See, e.g.*, New York *ex rel.* Banerjee v. Moody's Corp., 50 N.Y.S.3d 28 (N.Y. Sup. Ct. 2016); *In re* Stewart's Shops Corp., DTA No. 825745, 2016 WL 1086062, at *21 (N.Y. Div. Tax. App. Mar. 10, 2016);

> Addressing the second criterion, I find that the arrangement meets commonly accepted notions of insurance. Petitioner presented convincing evidence that BRIC was a bona fide insurance company. In forming BRIC, petitioner made a business decision premised on legitimate nontax considerations, including the desire to reduce insurance costs, obtain otherwise unavailable insurance coverage, increase incentive for risk management, and more efficiently manage and control its insurance program. BRIC was formed consistent with the New York Insurance Law and was licensed and regulated by the Insurance Department. Petitioner engaged PWC to assist in the formation and license application of BRIC, and to prepare a feasibility and actuarial study. In preparing the study, PWC reviewed petitioner's historic insurance policies and its loss history and proposed lines of insurance that BRIC should provide and amounts of premiums that should be charged for those lines on insurance. After BRIC was licensed, its captive manager finalized the lines of insurance BRIC would provide to petitioner, and determined the premiums to be charged based on the PWC study, petitioner's historical insurance needs and losses, market rates and industry standards for similar lines of insurance provided by other companies. At the end of each year, BRIC engaged AON to conduct an actuarial review of BRIC's operations. BRIC's captive manager annually reevaluated the lines of insurance and premiums based on the AON actuarial report, market rates and industry standards. BRIC reviewed and investigated claims submitted by petitioner, determined whether to approve or deny the claim, and paid claims from a separately maintained account. BRIC was adequately capitalized. Based on the foregoing, the evidence supports the conclusion that BRIC was a bona fide insurance company and the arrangement meets the commonly accepted notions of insurance.

In re Stewart's Shops Corp., DTA No. 825745, 2016 WL 1086062, at *21 (N.Y. Div. Tax. App. Mar. 10, 2016) (citations omitted).

whether this particular type of insurance—"residual value insurance"—was insurance.[73] Based on the state definitions, the court found the captive was insurance.[74] Impressively, the court—and only this court—referred to various insurance treatises to confirm that the insurance here was insurance.[75]

Except for *R.V.I.*, the preceding cases attempted to define insurance in the "commonly accepted sense." They started with an innocuous and vague statement from a life insurance and estate case, to accrete various non-technical ideas of insurance that resulted in a formal criterium for how tax law views insurance. This view of insurance differs from that of the insurance industry and insurance law.

IV. HOW INSURANCE VIEWS NOTIONS OF INSURANCE

An old law review Note on how insurance is defined, cited in *Allied Fidelity Corp.*,[76] cautioned on the efforts to classify insurance in different subjects:

> The meaning of the terms "insurance" and "insurance corporation" may differ considerably with the purposes for which the question is sought to be determined. Cases of one type may not be precedents for a case of a different type. In each case the purpose of the law involved, the powers and activities of the company, and the state's classification of the company, should be fully scrutinized to the end that the determinations in one field do not confuse the issues in another.[77]

As often happens, definitions are appropriate for core principles, but then practice outruns definitions and theory. Certainly, insurance involves

---

[73] *R.V.I. Guar. Co.*, 145 T.C. at 237–39.

[74] *Id.* at 246 ("Our analysis of insurance risk, risk transfer, risk distribution, and the commonly accepted notions of insurance convinces us that the RVI policies are 'insurance contracts' for Federal income tax purposes.").

[75] *Id.* at 240 (discussing 1 STEVEN PLITT, DANIEL MALDONADO, JOSHUA D. ROGERS & JORDAN PLITT, COUCH ON INSURANCE (3d ed. 2015) and NEW APPLEMAN ON INSURANCE LAW (Jeffrey E. Thomas et al. eds., Library ed. 2015)).

[76] Allied Fid. Corp. v. Comm'r, 66 T.C. 1068, 1073 (1976), *aff'd*, 572 F.2d 1190 (7th Cir. 1978).

[77] Note, *An Analysis of "Insurance" and "Insurance Corporation"*, 36 COLUM. L. R. 456, 472 (1936) (footnotes omitted).

risk transfer and risk distribution, and only corporations licensed and regulated as insurers can sell and transact insurance. Scholars and writers on insurance have long struggled to explain insurance beyond the core. This should induce caution by non-insurance practitioners and judges to not project their own common notions of what is insurance into the insurance field.

A. THE TREATISES TRY TO EXPLAIN WHAT IS INSURANCE

A review of many insurance treatises, old and new, finds some common definitions of insurance and then much resignation that the definitions do not always fit the practice. No definitions refer to "common notions of insurance" as a basis for concluding whether insurance is being practiced.

A well-known insurance treatise, *Couch on Insurance*, provides this statement on trying to define insurance:

> Insurance has been defined in numerous ways, but these variations are primarily semantic. Essentially, insurance is a contract by which one party (the insurer), for a consideration that usually is paid in money, either in a lump sum or at different times during the continuance of the risk, promises to make a certain payment, usually of money, upon the destruction or injury of "something" in which the other party (the insured) has an interest.[78]

This is the transfer of risk. "The primary requisite essential to a contract of insurance is the assumption of a risk of loss and the undertaking to indemnify the insured against such loss."[79] The treatise also looks to various definitions by the courts to add more aspects to the definitions.

> Other common definitions of insurance are (1) a contract to pay a sum of money upon the happening of a particular event or contingency; (2) indemnity for loss in respect of a specified subject by specified perils; (3) an undertaking by one party to protect another party from loss arising from

---

[78] 1 STEVEN PLITT, DANIEL MALDONADO, JOSHUA D. ROGERS & JORDAN R. PLITT, COUCH ON INSURANCE § 1:6 (3d ed., Westlaw, database updated Dec. 2021) (footnotes omitted).

[79] *Id.* § 1:9 (footnotes omitted).

> named risks, for the consideration and upon the terms and under the conditions recited; (4) a contractual security against anticipated loss where the risk of loss is occasioned by some future or contingent event and is shifted to or assumed by the insurer, with a distribution of the risk of loss by the payment of a premium or other assessment into a general fund; (5) a contract whereby one party promises for a consideration to indemnify the other against certain risks; and (6) a contract whereby one undertakes to indemnify another against loss, damage, or liability arising from an unknown or contingent event.[80]

Another standard modern insurance treatise is *Appleman on Insurance*, both the original and the current editions. The current edition, *New Appleman on Insurance Law*, has a fine essay on this topic by Robert H. Jerry, II, titled *What is Insurance*.[81] Jerry says "[t]hree concepts are central to an insurance contract: risk; risk transference; and risk distribution."[82] This analysis of insurance matches how the tax cases have defined insurance.

> A contract of insurance is an agreement in which one party (the insurer), in exchange for a consideration provided by the other party (the insured), assumes the other party's risk and distributes it across a group of similarly situated persons, each of whose risk has been assumed in a similar transaction. As this amplified definition indicates, insurance contracts involve an exchange of premium for the promise to assume risk, along with a distribution of the risk across similarly situated insureds. In this definition, "risk" connotes uncertainty in the sense that the loss must be one that is uncertain to occur or unpredictable and outside the substantial control of the parties to the contract.[83]

---

[80] *Id.* § 1:6 (footnotes omitted).

[81] Robert H. Jerry, II, *Defining Insurance, in* 1 NEW APPLEMAN ON INSURANCE LAW ch. 1 (Jeffrey E. Thomas & Francis J. Mootz eds., Library ed., LEXIS, database updated May 2022).

[82] *Id.* § 1.03[1].

[83] *Id.* § 1.03[2] (footnotes omitted).

Jerry then looks at state insurance statute definitions,[84] and a 1939 case,[85] to expand further on the position that indemnity alone is not insurance—there must be a "principal object and purpose" to transfer risk in exchange for a payment.[86] Jerry goes back to an earlier version of the *Appleman* encyclopedia for a way to define insurance.

> Courts should examine each commercial transaction to determine if the discrete transaction ought to be regulated in the public interest as the business of insurance. . . . Pursuant to this supplemental test, courts should minimally make the following inquiries.
>
> (1) What is the private interest sought to be protected in the commercial transaction? (Matters, such as insurable interest and risk of harm to that interest, under traditional definitions are evaluated here.)
>
> (2) Who is the party assuming the risk transferred? Is the protected interest indigenous to that party? (Arguably, there is more need for regulation if the assuming party is an independent, for-profit entity promising indemnity against certain risks to the insurable interest.)
>
> (3) Is the protected interest indigenous to the state and all its citizens? (Manifestly, a state and its citizens have a common indigenous interest in safety and health, including the delivery and quality of medical care, safe cars, well-built homes, and the like. Other interests may not be indigenous.)
>
> (4) Does the value of the indigenous interest invoke the purposes and policies of state insurance regulation for all its citizens? (Many reasons justify state insurance regulation, for example: to assure solvency, to assure fairness in rates and rating classifications, and to prevent contractual over-

---

[84] *See, e.g.*, CAL. INS. CODE § 22 (Deering, LEXIS through 2022 Reg. Sess.); W. VA. CODE ANN. § 33-1-1 (LEXIS through 2022 Legis.); KY. REV. STAT. ANN. § 304.1-030 (LEXIS through 2022 Legis.); WIS. STAT. ANN. § 600.03(25)(a) (LEXIS through 2021-2022 Legis.); MINN. STAT. ANN. § 60A.02 (LEIXS through 2022 Reg. Sess.); ME. REV. STAT. ANN. tit. 24-A, § 3 (LEXIS through 2021 First Reg. Sess.).

[85] Jordan v. Grp. Health Ass'n, 107 F.2d 239 (D.C. Cir. 1939).

[86] Jerry, *supra* note 81, § 1.03[3][b][ii].

> reaching. These concerns are addressed in this final question.)[87]

The prior *Appleman* series (to which Jerry refers) also had a chapter on defining insurance, and mostly gave up trying to do so, calling it "futile."[88]

> For competent insurance lawyering, one must understand that the subject has no useful, or fixed definition. There is neither a universally accepted definition or concept of "insurance" nor a exclusive concept or definition that can be pervasively applied in insurance lawyering. The question "What is Insurance?" arises in sundry lawyering operations and the contexts in which it arises may give rise to differing meanings. For instance, an evaluation of the discrete transaction's social and economic implications is usually significant in divining a definition. Moreover, the discrete circumstances may necessitate a more specialized definition. It would be foolhardy to state here what may seem to be a clear, comprehensive answer to the question: "What is Insurance?" As Learned Hand might observe, any universal definition for the term "insurance" would be "mythically prolix, and fantastically impractical." Thus, in our intricate and evolving commercial and social intercourse, it seems appropriate that any concept and meaning of insurance be sufficiently broad and flexible to meet the varying and innovative transactions which humankind perpetually produces. Understanding that the quest for a single, comprehensive definition is futile, let us undertake the quest to obtain the best comprehensive understanding we can.[89]

Thereafter, the discussion goes to risk and risk sharing.

---

[87] Jerry, *supra* note 81, § 1.03[3][b][iv] (quoting 1 ERIC MILLS HOLMES, APPLEMAN ON INSURANCE LAW & PRACTICE § 1.3 (2d ed., LEXIS, database updated Jan. 2010)).

[88] 1 HOLMES, *supra* note 87, § 1.3.

[89] *Id.*

> Risk sharing connotes not only a transfer of risk (risk-shifting) to others but a distribution (sharing) of the risk among the others. All contracts allocate and shift risks. An insurance contract differs from the ordinary contract because of risk distribution. In the insurance contract, the risk of an actual loss is distributed (socialized) among a large group of persons exposed to a comparable risk of loss.[90]

This sounds right, and relevant to captive insurance cases, except that the insured's transfer of risk to a commercial insurer does not actually distribute that risk to others; rather, that risk is held and borne by the commercial insurer. In a mutual insurer, it *might* be said that the risk is transferred to others. Or it can be more accurately said that the insured's risk is transferred to others only if the mutual insurer is an assessment mutual insurer that can charge back to the members any deficiency in capital to pay for an insured's loss.[91] A tax court example of this is *Commissioner v. Treganowan,* which found the New York Stock Exchange's gratuity fund that all members were required to pay in, and which would pay $20,000 death benefits for any member who died, was insurance.[92]

---

[90] *Id.*

[91] "Assessment mutual insurance companies do not require the policyholder to pay an advance premium; instead, the policyholder is liable to pay its share of the insurance company's losses and expenses at the end of each insurance period. Assessment mutual companies write a relatively small amount of insurance." 1 LINDA H. LAMEL, BUSINESS INSURANCE LAW AND PRACTICE GUIDE § 1.01[3][b] (LEXIS, database updated June 2022). "Assessment contracts are written either with limited or unlimited rights of assessment against the insureds. A member who belongs to an insurer in which liability is unlimited is bound to pay a proportional share of all the losses and legitimate expenses of the company." 3 PLITT, MALDONADO, ROGERS & PLITT, *supra* note 78, § 39:17. "A mutual insurance company is a cooperative enterprise wherein the policyholders, as members, are both insurer and insured. As members, each policyholder is liable for his proportionate share of indebtedness upon the insolvency of the company." Commonwealth v. Bankers Mut. Fire Ins. Co. of Lancaster, Pa., 45 Pa. D. & C.2d 558, 560–61 (Pa. C.P. 1968) (citations omitted).

[92] *See* Comm'r v. Treganowan, 183 F.2d 288, 291 (2d Cir. 1950):

> Here the risk of loss from premature death is effectively shifted from the individual to the group of other members of the Exchange. If the individual member dies prematurely, the amount

Similarly, in a risk retention group the risk is borne by others in the group.[93] The idea of risk distribution really means, then, that we all share in paying a small premium because everyone's small premium is available to pay for everyone else's occasional and actuarially-predicable loss.

After reviewing state statutes on the definition of insurance, *Appleman* concludes, "it is no facile matter to frame a definition which states accurately and plainly the common features of the enterprises that are generally regarded as subject to 'insurance' regulation."[94] Except, as *Appleman* concluded "[t]he rub is that such a definition may not be possible."[95]

In the next section, the author—after disclaiming the ability to define insurance "for universal application or state a conclusive test"[96]—proposes three dimensions to evaluate whether insurance exists in the transaction. The first dimension is the "substantial control test."[97]

> This traditional test was the earliest adopted by courts. The test conforms to the classical definition of insurance as an arrangement for transferring and distributing the risk of loss upon the happening of a fortuitous event. . . . The test derives from [a] . . . description of an insurance contract . . . as having the following five elements:
>
> (a) The insured possesses an interest of some kind susceptible to pecuniary estimation, and known as an insurable interest;

> paid in, the difference representing the loss caused by his premature death which the group has had to bear. Had he not been a member of the plan, he would have saved the amount of assessments against him before his death, but his beneficiaries would be $20,000 poorer. Thus they would have borne this loss which, through the Exchange plan, he has shifted to the group. And manifestly this plan provides a distribution of the risk, for because of the plan the risk of premature death is borne by the 1373 other members of the Exchange, rather than by the individual.

[93] *See, e.g.*, N.Y. INS. LAW § 5902 (McKinney, Westlaw through 2022 Legis.); CONN. GEN. STAT. § 38a-250 (West, Westlaw through 2022 Reg. Sess.).

[94] 1 HOLMES, *supra* note 87, § 1.3.

[95] *Id.*

[96] *Id.* § 1.4.

[97] *Id.*

> (b) The insured is subject to a risk of loss through the destruction or impairment of the insurable interest by the happening of certain designated fortuitous perils (today generally called the insured event);
>
> (c) The insurer assumes that risk of loss (which today we describe as risk transference);
>
> (d) The insurer assumes that risk as part of a general scheme to distribute actual losses among a large group bearing somewhat similar risks; and,
>
> (e) As consideration for the insurer's promise to assume the risk of loss, the insured makes a contribution (called a premium) to the general insurance fund ((d) and (e) constitute risk distribution).[98]

The second dimension to evaluate whether the transaction involves insurance is the "principal object or ancillary test."[99] "If 'insurance' is the dominant feature (the "basis of the bargain"), then the transaction ought to be defined and regulated as insurance. Contrawise, courts will tolerate a marginal, 'insurance kicker' element, provided that element is relatively insignificant and incidental to the principal objective of the commercial transaction."[100] That means, "[i]n sum, the generally prevailing test today starts with the control (fortuitous) test and then evaluates the insurance element to determine if it is marginal (incidental, ancillary) or predominant."[101]

The third dimension to use is the "regulatory value test," meaning, "[c]ourts should examine each commercial transaction to determine if the discrete transaction ought to be regulated in the public interest as the business of insurance."[102]

As to principal purpose, consider extended warranty and home protection contracts (also known as home warranty contracts) as examples of what the contract really is about. These contracts promise to make repairs to a vehicle or a home and its appliances in exchange for a fixed annual fee. The California legislation specifies that the commercial contracts are not insurance but are their own class of home protection companies licensed as

---

[98] *Id.* (footnote omitted).
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*

such,[103] and this comports with the standard purpose of insurance to pay for a loss, not to do actual repairs.[104] Florida also views home warranty contracts as distinct from insurance.[105] In contrast, Virginia seems to interpret these types of contracts as insurance.[106] *Couch on Insurance* says:

> In some states, the legislature has specifically amended the relevant statutes to bring automobile dealers offering extended service contracts within the scope of state insurance regulators. As a general statement, a warranty that covers the goods sold for defects that likely existed in the goods at the time of sale is not an insurance contract, while a warranty that goes materially beyond the goods, or beyond defects in the goods, to compensate for losses due to causes

---

[103] CAL. INS. CODE § 12744 (Deering, LEXIS through 2022 Reg. Sess.); CAL. INS. CODE § 12745 (Deering, LEXIS through 2022 Reg. Sess.).

[104] *See* CAL. INS. CODE § 12740(a) (Deering, LEXIS through 2022 Reg. Sess.):

> "Home protection contract" means a contract or agreement whereby a person, other than a builder, seller, or lessor of the home which is the subject of the contract, undertakes for a specified period of time, for a predetermined fee, to repair or replace all or any part of any component, system or appliance of a home necessitated by wear and tear, deterioration or inherent defect, arising during the effective period of the contract, and, in the event of an inspection conducted pursuant to subdivision (b) of Section 12761, by the failure of that inspection to detect the likelihood of any such loss.

The court in Chu v. Old Republic Home Prot. Co., 274 Cal. Rptr. 3d 528, 532 (Ca. Ct. App. 2021), *reh'g denied (*Ca. Ct. App. 2021), *rev denied* (Ca. Ct. App. 2021), recounted the history of this statute:

> The initial draft of the senate bill . . . would provide for the regulation of persons engaged in the sale of home maintenance contracts '*as insurers*, subject to specified provisions of the Insurance Code.' . . .
>
> The final version of the bill . . . however, deleted the references to insurers and insurance, and instead referred to home maintenance or warranty contracts as 'home protection contracts.'

[105] FLA. STAT. ANN. § 634.301 (West, Westlaw through 2022 Reg. Sess.).

[106] VA. CODE ANN. § 38.2-2613 (LEXIS through 2022 Reg. Sess.); VA. CODE ANN. § 38.2-129 (LEXIS through 2022 Reg. Sess.).

> unrelated to the general merchantability of the goods is an insurance contract. . . .
>
> . . .
>
> Even a warranty that does extend to losses beyond defects in the product itself may escape characterization as insurance if the element of "risk transfer" involved is sufficiently incidental to the primary purpose of the contract.[107]

It may also be useful to compare this concept with the determination of whether a contract is for the sale of goods sufficient to come within the Uniform Commercial Code ("UCC") or a sale of services where the goods are ancillary. When the dominant purpose of a contract is the sale of goods, the UCC applies.[108]

The National Association of Insurance Commissioners defines insurance as "an economic device transferring risk from an individual to a company and reducing the uncertainty of risk via pooling."[109] Similarly, the Commission on Insurance Terminology of the American Risk and Insurance Association in 1965 defined insurance as "the pooling of fortuitous losses by transfer of such risks to insurers, who agree to indemnify insureds for such

---

[107] 1 PLITT, MALDONADO, ROGERS & PLITT, *supra* note 78, § 1:20 (footnotes omitted).

[108] *See, e.g.*, KSW Mech. Servs. v. Johnson Controls, Inc., 992 F. Supp. 2d 135, 141 (E.D.N.Y. 2014) ("Contracts for goods which involve—incident to the sale of goods—services such as installation, maintenance, testing, instruction or supervision are still subject to the UCC."); Accessory Overhaul Grp., Inc. v. Mesa Airlines, Inc., 994 F. Supp. 2d 1296, 1301 (N.D. Ga. 2014) ("When the predominant element of a contract is the sale of goods, the contract is viewed as a sales contract and the UCC applies, even though a substantial amount of service is to be rendered in installing the goods."); Belleville Toyota, Inc. v. Toyota Motor Sales, U.S.A., Inc., 770 N.E.2d 177, 194 (Ill. 2002) ("Where, as here, a contract provides both for the sale of goods and for the rendition of services, Illinois courts apply the 'predominant purpose' test in determining whether the contract falls within article 2 of the UCC."); Allied Shelving & Equip., Inc. v. Nat'l Deli, LLC, 154 So. 3d 482, 484 (Fla. Dist. Ct. App. 2015) ("In such instances, the determination whether the "predominant factor" in the contract is for goods or for services is a factual inquiry unless the court can determine that the contract is exclusively for goods or services as a matter of law."); Wall St. Network, Ltd. v. N.Y. Times Co., 80 Cal. Rptr. 3d 6, 19 (Ca. Ct. App. 2008).

[109] *Glossary of Insurance Terms*, NAIC, https://content.naic.org/consumer_glossary#I (last visited Mar. 14, 2022).

losses, to provide other pecuniary benefits on their occurrence, or to render services connected with the risk."[110] These ideas of pooling are more useful than the standard statement about risk distribution, which has conceptual and implementation problems discussed later.[111]

In summary, in reviewing the major treatises on insurance, we should say that if there are any "commonly accepted notions of insurance" in the insurance field, the *Appleman* test might be it: (1) substantial control test, meaning an exposure to loss and the actual transfer of risk; (2) principal object or ancillary test, meaning the point of the contract is to obtain insurance, not something else that may include an insurance component; (3) regulatory value test, meaning there is a public interest in regulating this activity as insurance.[112]

Earlier insurance treatises are informative but no more definitive on a common notion of insurance. Joseph K. Angell, in *A Treatise on the Law of Fire and Life Insurance,* states:

> A more general definition is, a contract by which one of the parties binds himself to the other, to pay him a sum of money, or otherwise *indemnify* him, in the case of the happening of a fortuitous event provided for in a general or special manner in the contract, in consideration of the sum of money which the latter pays, or binds himself to pay him. It is a contract to protect men against uncertain events which *in any wise* may be a disadvantage to them.[113]

Robert Riegel and Jerome S. Miller in *Insurance Principles and Practices* state:

> Insurance is pre-eminently social in nature. It represents, in the highest degree, co-operation for mutual benefit. Various individuals who are all subject to similar risks combine to reduce the consequences of these risks, many thousands of persons paying premiums in order that the unfortunate few may be indemnified for the losses that

---

[110] GEORGE E. REJDA & MICHAEL J. MACNAMARA, PRINCIPLES OF RISK MANAGEMENT AND INSURANCE 20 (Donna Battista et al. eds., 12th ed. 2014).

[111] *See infra* Part I and Part VII.

[112] 1 HOLMES, *supra* note 87, § 1.4.

[113] JOSEPH K. ANGELL, A TREATISE ON THE LAW OF FIRE AND LIFE INSURANCE 3 (Boston, Little, Brown & Co. 2d ed. 1855) (footnotes omitted).

> will occur. This principle of mutuality is present in a "stock company" organized for profit, as well as in a "mutual company," because in the last analysis losses are paid from premiums.[114]

Allen H. Willett, in *The Economics Theory of Risk and Insurance,* defines insurance "as that social device for making accumulations to meet uncertain losses of capital which is carried out through the transfer of the risks of many individuals to one person or to a group of persons."[115]

Robert I. Mehr and Emerson Cammack in *Principles of Insurance* state:

> Insurance itself may be defined as a social device for reducing risk by combining a sufficient number of exposure units to make their individual losses collectively predictable. The predictable loss is then shared proportionately by all those in the combination. This definition implies *both* that uncertainty is reduced and that losses are shared. These are the important essentials of insurance.
>
> From the point of view of the individual insured, insurance is a device that makes it possible for him to substitute a small, definite cost (the premium) for a large but uncertain loss (up to the amount of the insurance) under an arrangement whereby the fortunate many who escape loss will help to compensate the unfortunate few who suffer loss.[116]

Frank Joseph Angell in *Insurance Principles and Practices* states that insurance can be defined from a legal standpoint as a contract; from a social standpoint "as a method of combining a large enough group of units to make the loss predictable. . . . [T]o enable[] the individual to obtain insurance at a reasonable rate and thus to protect himself against the

---

[114] ROBERT RIEGEL & JEROME S. MILLER, INSURANCE PRINCIPALS AND PRACTICES 23 (3d ed. 1947).

[115] ALLAN H. WILLETT, THE ECONOMIC THEORY OF RISK AND INSURANCE 72 (1951).

[116] ROBERT I. MEHR & EMERSON CAMMACK, PRINCIPLES OF INSURANCE 33–34 (3d ed. 1961).

possibility of disastrous losses;" and from an accounting standpoint "as a method of substituting a small certain loss for a large uncertain loss."[117]

Neil A. Doherty, a professor of insurance at the Wharton School, gave this definition in a case on captive insurance: "[a]n institution whereby a number of individuals or firms transfer their premiums and their exposures to loss to a common fund, and the common fund is then available to pay for the losses of whoever might suffer them."[118] The court further noted that Doherty stated that "the risk dimension that is being transferred is the unpredictability or variability of loss and not the expected loss or long run average cost.[119]

This leaves us with a variety of definitions of insurance, none of which can be said to be common notions. As with many things, the more we try to define something, the more difficult we find a definition to be, while more people seem to think they know it when they see it. If the insurance treatises and insurance cases struggle to define insurance, it should generate

---

[117] FRANK JOSEPH ANGELL, INSURANCE PRINCIPLES AND PRACTICES 3 (1959) (italics omitted). These ideas of insurance as a social aspect were taken in a different direction, viewing "insurance companies as voluntary associations, alternative to the state, which provide social benefits." Carol Weisbrod, *Insurance and the Utopian Idea*, 6 CONN. INS. L.J. 381, 384 (2000). The author notes connections between religion and insurance, which we could more accurately restate as being the fraternal associations and reciprocal exchanges that later were classified as insurance:

> The idea of insurance as compensation for losses resulting from various ascertainable risks can be viewed as building on utopian security goals. The questions in their largest formulation involve the relation between freedom and security. In contract terms, the questions relate to the idea of solidarity and the nature of the commitments which individuals make to each other, whether a commitment is to a global framework or to a legal system which recognizes individual insurance contracts.
>
> The utopian idea has a clear connection to fraternal organizations as providers of insurance, as it does to the history of immigration and the attempts by social agencies to assist them. Both the insurance agent and the "friendly visitor" (as well, one assumes, as the parish priest) visited the homes of the poor.
>
> But it is also linked to the history of these independent insurance companies that stressed service goals.

Id. at 402–03 (footnotes omitted).

[118] Ocean Drilling & Expl. Co. v. United States, 24 Cl. Ct. 714, 727 (1991), *aff'd*, 988 F.2d 1135 (Fed. Cir. 1993).

[119] *Id.*

strong doubts that the tax cases can assume, adopt, or declare commonly accepted notions of insurance.

B. STATE INSURANCE STATUTES DEFINE INSURANCE, MORE OR LESS

State statutory definitions are generic statements of insurance. More importantly, the tax court cases that specify factors for commonly accepted notions of insurance are nowhere within those definitions. Here are a few such statutes:

California:

> "Insurance is a contract whereby one undertakes to indemnify another against loss, damage, or liability arising from a contingent or unknown event."[120]

Connecticut:

> (11) "Insurance" means any agreement to pay a sum of money, provide services or any other thing of value on the happening of a particular event or contingency or to provide indemnity for loss in respect to a specified subject by specified perils in return for a consideration. In any contract of insurance, an insured shall have an interest which is subject to a risk of loss through destruction or impairment of that interest, which risk is assumed by the insurer and such assumption shall be part of a general scheme to distribute losses among a large group of persons bearing similar risks in return for a ratable contribution or other consideration.
>
> (12) "Insurer" or "insurance company" includes any person or combination of persons doing any kind or form of insurance business other than a fraternal benefit society, and shall include a receiver of any insurer when the context reasonably permits.[121]

---

[120] CAL. INS. CODE § 22 (Deering, LEXIS through 2022 Reg. Sess.).
[121] CONN. GEN. STAT. § 38a-1 (West, Westlaw through 2022 Reg. Sess.).

Massachusetts:

> "A contract of insurance is an agreement by which one party for a consideration promises to pay money or its equivalent, or to do an act valuable to the insured, upon the destruction, loss or injury of something in which the other party has an interest."[122]

New York:

> "Insurance contract" means any agreement or other transaction whereby one party, the "insurer", is obligated to confer benefit of pecuniary value upon another party, the "insured" or "beneficiary", dependent upon the happening of a fortuitous event in which the insured or beneficiary has, or is expected to have at the time of such happening, a material interest which will be adversely affected by the happening of such event.[123]

A California case interpreting the California statute, and relying on cases from around the country to explain insurance, quoted this explanation:

> Whether the contract is one of insurance or of indemnity . . . there must be a risk of loss to which one party may be subjected by contingent or future events and an assumption of it by legally binding arrangement by another. Even the most loosely stated conceptions of insurance and indemnity require these elements. Hazard is essential and equally so a shifting of its incidence. If there is no risk, or there being one it is not shifted to another or others, there can be neither insurance nor indemnity. Insurance also, by the better view, involves distribution of the risk, but distribution without assumption hardly can be held to be insurance.[124]

---

[122] MASS. GEN. LAWS ANN. ch. 175 § 2 (West, Westlaw through 2022 2nd Annual Sess.).

[123] N.Y. INS. LAW § 1101 (McKinney, Westlaw through 2022 Legis.).

[124] Cal. Physicians' Serv. v. Garrison, 172 P.2d 4, 12 (Cal. 1946) (quoting Jordan v. Grp. Health Ass'n, 107 F.2d 239, 245 (D.C. Cir. 1939)).

V. COMPARING INSURANCE NOTIONS AGAINST TAX NOTIONS OF INSURANCE

The tax court decisions that have spawned their own commonly accepted notions of insurance do not all square with the insurance practice and law's notions of insurance. These decisions and treatises are compiled in the table below.

Reserve Mechanical[125]	***Securitas Holdings***[126]
1. "[W]hether it was created for legitimate nontax reasons; 2. whether there was a circular flow of funds; 3. whether the entity faced actual and insurable risk; 4. whether the policies were arm's-length contracts; 5. whether the entity charged actuarially determined premiums; 6. whether comparable coverage was more expensive or even available; 7. whether it was subject to regulatory control and met minimum statutory requirements; 8. whether it was adequately capitalized; and 9. whether it paid claims from a separately maintained account."	1. "[T]he insurer was organized, operated, and regulated as an insurance company; 2. the insurer was adequately capitalized; 3. the insurance policies were valid and binding; 4. the premiums were reasonable; and 5. the premiums were paid and the losses were satisfied."

[125] Rsrv. Mech. Corp. v. Comm'r, 115 T.C.M. (CCH) 1475, 2018 T.C.M. (RIA) ¶ 2018-086, slip op. at 38–39 (2018), *appeal docketed*, No. 18-9011 (10th Cir. Dec. 27, 2018).

[126] Securitas Holdings, Inc. v. Comm'r, 108 T.C.M. (CCH) 490, 2014 T.C.M. (RIA) ¶ 2014-225, slip op. at 27 (2014).

New Appleman on Insurance Law[127]	***Appleman On Insurance Law & Practice***[128]
1. "What is the private interest sought to be protected in the commercial transaction? . . . 2. Who is the party assuming the risk transferred? Is the protected interest indigenous to that party? . . . 3. Is the protected interest indigenous to the state and all its citizens? . . . 4. Does the value of the indigenous interest invoke the purposes and policies of state insurance regulation for all its citizens?"	1. Substantial control; 2. Principal object and ancillary; and 3. Regulatory value

Some of the tax court questions are useful and relevant when examining instances that resemble insurance, and many are useful for examining the financial and economic substance of the transactions between the parent corporation and its subsidiary. However, that does not make them instances of proving insurance in practice. Certainly, the tax courts and the IRS should ask whether a captive insurer was formed for a legitimate non-tax purpose (this goes with the *Appleman* test of principal object and purpose),[129] and whether there was a circular flow of funds (as posited in *Reserve Mechanical* factor 2).[130] Certainly, the premiums should be actuarially based (as posited in *Reserve Mechanical* factor 5).[131]

Thereafter, the tax courts' view of commonly accepted notions fail as insurance notions. *Reserve Mechanical* factor 4 (for arms-length transactions)[132] will be problematic in assessing the independence of a subsidiary corporation. Until the twentieth century, a corporation could not

---

[127] Jerry, *supra* note 81, § 1.03[3][b][iv].
[128] 1 HOLMES, *supra* note 87, § 1.4.
[129] *See supra* notes 99–01, 128 and accompanying text.
[130] *See supra* note 125 and accompanying text.
[131] *Id.*
[132] *Id.*

even hold the shares of a subsidiary corporation unless the legislative grant of the corporate charter specifically allowed it.[133] There may, of course, be finance and control issues that undercut a legitimate business of the subsidiary, and which denigrate, if not collapse, the separate corporate legal entity of the subsidiary. Meanwhile, practical and economic realities of the relationship between a subsidiary and its parent will always evince the links of some corporate control, like members of the parent having some board seats on the subsidiary and the reality of consolidated financial statements. That does not deny the separate legal existence of a subsidiary,[134] nor make it contradict a notion of insurance. Further, if transactions within a corporate group are viewed as a whole, then every transaction would fail to survive the business purpose test.[135] Thus, some false notion of insurance cannot be the reason to disregard the transaction.

Reserve Mechanical factors 7, 8, and 9[136] seem inherent to insurance regulation: if a state regulator or off-shore domicile regulator says the company is an insurance company in good standing, then that should end the

---

[133] *See* JAMES C. BONBRIGHT & GARDINER C. MEANS, THE HOLDING COMPANY: ITS PUBLIC SIGNIFICANCE AND ITS REGULATION 55–58 (New York, Augustus M. Kelly 1st ed. 1969). *See also* Kateena O'Gorman, *Remembering the Concept of the Corporation*, white paper presented at the Stanford/Yale Junior Faculty Forum, May 29, 2009, at 13–19; 6A WILLIAM MEADE FLETCHER ET AL., CYCLOPEDIA OF THE LAW OF CORPORATIONS §§ 2825-26 (Thomson Reuters ed., Westlaw, database updated Apr. 2022); William Randall Compton, *Early History of Stock Ownership by Corporations*, 9 GEO. WASH. L. REV. 125, 130–32 (1940); Phillip I. Blumberg, *Limited Liability and Corporate Groups*, 11 J. CORP. L. 573, 575 n.2, 606–11 (1986); Note, *Power of a Corporation to Acquire Stock of Another Corporation*, 31 COLUM. L. REV. 281, 281–85, 288–89 (1931). Of note, Bonbright & Means contend that in 1888, New Jersey became the first state to allow a corporation to hold shares of a subsidiary corporation. BONBRIGHT & MEANS, *supra* note 133, at 55. However, Fred Freedland argues that New York was the first jurisdiction to grant the general right for one corporation to own share of another, in 1853, for life and health insurers, and thereafter for other insurers, banks and railroad corporations. Fred Freedland, *History of Holding Company Legislation in New York State: Some Doubts as to the "New Jersey First" Tradition,* 24 FORDHAM L. REV. 369, 370–77 (1955).

[134] *See* Bobby L. Dexter, *Rethinking "Insurance," Especially After AIG*, 87 DENV. U. L. REV. 59, 76 (2009).

[135] *See* Donald Arthur Winslow, *Tax Avoidance and the Definition of Insurance: The Continuing Examination of Captive Insurance Companies*, 40 CASE W. RSRV. L. REV. 79, 118 (1989).

[136] *See supra* note 125 and accompanying text.

tax inquiry on that point.[137] One author stated the point as: "insurance is what regulators allow insurers to do."[138] Unless there is a basis to call the captive insurance company a corporate sham or operating illegally[139]—which sometimes may be the case—there is little a court should do with *Reserve Mechanical* factors 7 and 8[140] as to deciding insurance. If the court does find a corporate sham, then the problem needs to be referred to the appropriate regulator.

Reserve Mechanical factor 9 (whether claims were funded from a separately maintained account)[141] was essentially rejected in a California insurance case. "Whether an entity is an insurer does not depend on the entity's size, sophistication, corporate retention policies, or claims handling abilities."[142] The court then looked at the California insurance statutes and the "principal object and purpose" test to determine whether the contract constituted insurance.[143]

Reserve Mechanical factor 6 (whether comparable coverage was more expensive or even available)[144] presents several problems. As to price, this has nothing to do with any notion or definition of insurance. Whether to pay more, or too much, is a purchaser's decision, not a seller's decision. There is no insurance law that requires a buyer to avoid expensive insurance. There may actually be some legitimate reasons to pay more for insurance, such as (1) the expensive insurer provides a package of coverages and policies that might be too hard to put together from several insurers and might create gaps in coverage; (2) risk control services might be provided

---

[137] *See, e.g.*, *In re* Stewart's Shops Corp., DTA No. 825745, 2016 WL 1086062 (N.Y. Div. Tax. App. Mar. 10, 2016) (New York-licensed captive); Malone & Hyde, Inc. v. Comm'r, 62 F.3d 835 (6th Cir. 1995) (Colorado-licensed captive); Kiddie Indus., Inc. v. United States, 40 Fed. Cl. 42, 51 (Fed. Cl. 1997), *dismissed*, 194 F.3d 1330 (Fed. Cir. 1999) (Bermuda-licensed captive); R.V.I. Guar. Co. & Subsidiaries v. Comm'r, 145 T.C. 209 (2015) (Connecticut-licensed captive).

[138] Christian Thimann, *What is Insurance and How Does it Differ from General Finance?*, *in* THE ECONOMICS, REGULATION, AND SYSTEMIC RISK OF INSURANCE MARKETS 5, 13 (Felix Hufeld, Ralph S. J. Koijen, & Christian Thimann eds., 2017).

[139] *See, e.g.*, Ocean Drilling & Expl. Co. v. United States, 24 Cl. Ct. 714, 728–29 (1991), *aff'd*, 988 F.2d 1135 (Fed. Cir. 1993) (analyzing if the corporation was a sham).

[140] *See supra* note 125 and accompanying text.

[141] *Id.*

[142] Truck Ins. Exch. v. Amoco Corp., 41 Cal. Rptr. 2d 551, 556 (Cal. Ct. App. 1995).

[143] *Id.* (reviewing CAL. INS. CODE §§ 22–23 (Deering, LEXIS through 2022 Reg. Sess.)).

[144] *See supra* note 125 and accompanying text.

and thus justify a higher price; and (3) a hardening market may motivate the decision to remain with a long-standing carrier rather than switch. If, in fact, the price for the insurance is far out of line with what is commercially available, then this goes to a management failure for waste of corporate assets, for which the remedy is a shareholder action (even a private corporation may use this remedy) or a state attorney general investigation.[145]

As to the availability of coverage under *Reserve Mechanical* factor 6,[146] this too does not define insurance. The insurance industry has multiple ways to provide unique coverages, mostly through the surplus lines markets, which specialize in providing one-off coverages.

> Surplus lines insurance is property and casualty coverage that is underwritten by a non-admitted insurer for nonstandard risks or policy levels that are unavailable in the commercial market. Policies may not be issued through the surplus lines market without a licensed surplus lines broker pursuing the coverage in the admitted market, without success.[147]

---

[145] *See* 16A FLETCHER ET AL., *supra* note 133, § 8068.10; N.Y. BUS. CORP. LAW § 720 (McKinney, Westlaw through 2022 Legis.); Michelson v. Duncan, 407 A.2d 211, 217 (Del. 1979) ("The essence of a claim of waste of corporate assets is the diversion of corporate assets for improper or unnecessary purposes.");

> [W]e have defined "waste" to mean "an exchange of corporate assets for consideration so disproportionately small as to lie beyond the range at which any reasonable person might be willing to trade." As a practical matter, a stockholder plaintiff must generally show that the board "irrationally squander[ed]" corporate assets—for example, where the challenged transaction served no corporate purpose or where the corporation received no consideration at all.
>
> Under this standard, a corporate waste claim must fail if "there is *any substantial* consideration received by the corporation, and . . . there is a *good faith judgment* that in the circumstances the transaction is worthwhile."

White v. Panic, 783 A.2d 543, 554 (Del. 2001) (citations omitted).

[146] *See supra* note 125 and accompanying text.

[147] Julie Mix McPeak, *Regulation of Non-Admitted Market/Surplus Lines, in* 2 NEW APPLEMAN ON INSURANCE LAW § 9.09[1] (Jeffrey E. Thomas & Martin F. Grace eds., Library ed., LEXIS, database updated May 2022).

This is the reason for, and often the realm of, surplus lines insurers, to develop and underwrite insurance for unusual or evolving risks.

> Surplus lines insurers mainly focus on the development of new coverages and the structuring of policies and premiums appropriate for risks. New and innovative insurance products for which there is no loss history are difficult, if not impossible, to appropriately price using common actuarial methods. Often, after a new coverage has generated sufficient data, the coverage eventually becomes a standard product in the admitted market.[148]

How much effort does an insured, its broker, and the surplus lines broker, put into such a search for comparable coverages and prices to decide whether a captive is an appropriate alternative? Whatever the answer, there is almost always a surplus lines insurer that can underwrite the risk (after appropriate compliance with the surplus lines brokerage requirements).[149] The best known of the surplus insurers is the Lloyds of London syndicates, which essentially will cover anything.[150] This means that the question of whether an insurer would be willing to write a unique coverage is a flawed basis for determining whether a captive is insurance in the commonly

---

[148] *Surplus Lines*, NAT'L ASS'N OF INS. COMM'RS: CTR. FOR INS. POL'Y & RSCH. https://content.naic.org/cipr_topics/topic_surplus_lines.htm (Oct. 14, 2021). "As of year-end 2018, surplus lines direct premium volume was $49.9 billion representing 7.4% of the $676.6 billion of total U.S. direct premiums written. Although the surplus lines premium seems minimal compared to the total, in the absence of this market, many insureds would be unable to secure coverage." *Id*.

[149] *See, e.g.*, CAL. INS. CODE § 1763 (Deering, LEXIS through 2022 Reg. Sess.); N.Y. INS. LAW § 2118 (McKinney, Westlaw through 2022 Legis.); 15 U.S.C.A. § 8204; NAT'L ASS'N OF INS. COMM'RS, NONADMITTED INSURANCE MODEL ACT (2002), https://content.naic.org/sites/default/files/inline-files/MDL-870.pdf. *See generally* McPeak, *supra* note 147 ("State insurance departments regulate surplus lines insurers through eligibility determinations to participate in the surplus lines market within the state. However, surplus lines brokers are extensively regulated by state insurance departments through initial licensure, due diligence searches, reporting obligations and remittance of taxes. The insurance commissioner requires a surplus lines agent to determine the scope and availability of coverage in the admitted market and the eligibility of the surplus lines insurer prior to placing the insurance coverage.").

[150] *See generally What Lloyd's Insures*, LLYOD'S, https://www.lloyds.com/about-lloyds/what-we-insure (last visited Apr. 22, 2022).

accepted sense. Unless a state insurance statute or regulation says that insurance is illegal, it is probably available.

Indeed, pushing this question only a little further raises serious questions about the element of risk distribution, which is usually (but not always) based on a large number of homogenous units. The advantage of having a large number of homogenous units is that it allows for probability determinations of losses, and thus prices for those similar exposures.[151] That is the case for standard lines of insurance and sometimes for surplus lines of insurance, such as windstorm and even private flood risks, where the peril or exposure is common—but the admitted insurers decline to insure against catastrophic losses. That is sometimes *not* the case for surplus lines of insurance, such as insuring satellite launches,[152] the first offshore wind farms, cryogenic human storage, pollution sites, and computer networks in

---

[151] *See* Neil A. Doherty, *The Design of Insurance Contracts When Liability Rules are Unstable*, 58 J. RISK & INS. 227, 229 (1991) ("From the law of large numbers it is known that an insurance market with a large number of independent exposures will substantially reduce portfolio risk."). *See also* ANGELL, *supra* note 117, at 19 ("The law of large numbers may be defined as follows: The greater the number of exposure units, the nearer the actual results will approach the underlying probability." (italics omitted)); 1 JEFFREY W. STEMPLE & ERIK S. KNUTSEN, STEMPEL AND KNUTSEN ON INSURANCE COVERAGE § 1.03[A] (4th ed. 2020); REJDA & MCNAMARA, *supra* note 110, at 20–21.

[152] Piotr Manikowski & Mary A. Weiss, *The Satellite Insurance Market and Underwriting Cycles*, 38 GENEVA RISK & INS. REV. 148, 170 (2013) ("Recall that this line does not benefit from the law of large numbers relative to most other insurance lines with respect to homogeneity of data. Hence data for several periods as well as considerable judgment may enter the rating process leading to a longer cycle period."). The articles notes that the first insurance policy on a satellite was in 1965, and that (as of 2013) there are usually no more than thirty launches a year though losses can exceed $250 million, thus several insurers will subscribe to one launch. *Id.* at 152–54. As to setting the premium, "rates have been set in reaction to claims experience (recent market experience), rather than by statistical analysis of the launch and in-orbit record." *Id.* at 158 (citation omitted). This indicates insufficient data to predict probabilities, or at least insufficient use of and credibility of the limited data. The point is also made in Neil A. Doherty, *Risk-Bearing Contracts for Space Enterprises*, 56 J. RISK & INS. 397, 401 (1989) ("First, satellite insurance pools are small. . . . In recent years, the number of insured launches per year was 20 or less. Moreover, these were not all covered by all underwriters. Thus, each underwriter has carried only a handful of coverages in any year. This is an insufficient base from which to diversify risk effectively.") But the lack of diversification due to few insured exposures in satellite launches is diversified by the insurer's portfolio of aviation risks. *Id.*

cyber insurance.[153] Even contests with payouts, such as to capture the Loch Ness Monster for a £1,000,000 prize[154] or a hole-in-one in golf are insured.[155]

Some of these were one-of-a-kind or rare exposures, until they became common enough to price with some experience, and more common later to move into the standard lines where they meet a tax court's idea of what is common notions of insurance. Surplus lines insurers regularly take

---

[153] A specialty brokerage in Atlanta, INSUREtrust, created the first cyber policy in 1997. Andrea Wells, *What Agent Wrote First Cyber Policy Thinks About Cyber Insurance Now,* INS. J. (Mar. 1, 2018), https://www.insurancejournal.com/news/national/2018/03/01/481886.htm; Brian D. Brown, *The Ever-Evolving Nature of Cyber Insurance,* INS. J. (Sept. 22, 2014), https://www.insurancejournal.com/magazines/mag-features/2014/09/22/340633.htm. *See also INSUREtrust: Cyber Insurance & Risk Management Leader*, ENTER. SEC., https://risk-and-compliance-management.enterprisesecuritymag.com/vendors/insuretrust/2021 (last visited Apr. 23, 2022).

[154] ANTONY BROWN, LLOYD'S OF LONDON 154 (1974). The premium was £2,500, the policy period was one year from May 1, 1971, and provided the following coverage, written in all capital letters:

> THIS POLICY IS TO PAY £1,000,000 IN THE EVENT OF THE LOCH NESS MONSTER BEING CAPTURED ALIVE (UNDER THE RULES OF A COMPETITION RUN BY CUTTY SARK) IN LOCH NESS BETWEEN 1ST MAY, 1971, AND 30TH APRIL, 1972. AS FAR AS THIS INSURANCE IS CONCERNED THE LOCH NESS MONSTER SHALL BE DEEMD TO BE: -
> 1) IN EXCESS OF 20 FEET IN LENGTH
> 2) ACCEPTABLE AS THE LOCH NES MONSTER TO THE CURATORS OF THE NATURAL HISTORY MUSEUM, LONDON,
>
> IN THE EVENT OF LOSS HEREUNDER: -
> A) THE MONSTER SHALL BECOME THE PROPERTY OF UNDERWRITERS HEREON.
> B) IMMEDIATE NOTICE TO BE GIVEN TO UNDERWRITERS HEREON.

Photograph of Lloyd's Loch Ness Monster Insurance Policy, *in* ANTONY BROWN, LLOYD'S OF LONDON (1974), following p. 146.

[155] Hole-in-one insurance for golf tournaments would not seem to fit anyone's idea of a commonly accepted notion of insurance, but it is insurance. *See, e.g.*, Golf Mktg. Worldwide, LLC v. State Ins. Dep't, No. CV020523382S, 2004 Conn. Super. LEXIS 926 (Conn. Super. Ct. 2004) (finding that paying a contract price to cover the risk of paying out cash or a new automobile as prizes for scoring a hole in one constitutes insurance).

one-off types of risks with little historical data for pricing.[156] That does not in any way reduce the risk transfer from insured to insurer, nor contrary to the tax court decisions that contend a captive insurer for a one-off risk. It does make the prediction of loss more of a gamble. But the unpredictable losses on the small line of insured risks (such as satellites) are diversified by the insurer's overall portfolio, creating cross-pooling. "Thus the satellite risks can be, and are, pooled with all other business. This 'cross line pooling' can dramatically reduce the overall risk to the firm if the cross line correlations are low."[157] That is risk transfer, and that is the object and purpose of the transaction; thus fully qualifying the event as insurance.

The insurance market also provides political risk coverage, tax liability insurance, transaction representation and warranty insurance, credit receivables insurance, event cancellation insurance, film completion insurance, and specialized insurance on athletes (a type of disability insurance)–to name a few. Outside of the insurance and risk industries, few people would think of these as insurance. Yet, within the insurance and risk industries, these are known among the specialists who deal with these exposures.

Beyond surplus lines, the insurance industry goes even further with "alternative risk transfer" to deal with the most unique exposures.[158] This is insurance, too.

In sum, the tax courts' view of factors constituting "commonly accepted notions of insurance" mostly does not align with the insurance industry's views of notions of insurance. Actually, some of those factors do not even deal with insurance; they deal more with corporate law and corporate governance. As one author stated at the start of the captive-tax collision in 1990: "problems present in the captive context are best dealt with by other solutions, and not by manipulating the definition of insurance."[159] The author observed that "tax authorities, purporting to base their decisions

---

[156] *See* Shawn Moynihan, '*Specialty" Treatment': The State of the E&S Market.* PROP. CAS. 360 (Sept. 08, 2017, 2:30 AM), https://www.propertycasualty 360.com/2017/09/08/specialty-treatment-the-state-of-the-es-market/.

[157] Doherty, *supra* note 152, at 401.

[158] *See, e.g.*, Jens Peters, *What is Alternative Risk Transfer?*, WILLIS TOWERS WATSON (Aug. 17, 2017), https://www.willistowerswatson.com/en-US/insights/ 2017/08/what-is-alternative-risk-transfer; ALLIANZ GLOBAL CORPORATE & SPECIALTY SE, SALES APPETITE: ALTERNATIVE RISK TRANSFER AT A GLANCE (2021), https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/ countries/agcs-usa/marketing-brochures/AGCS-North-America-Alternative-Risk-Transfer-At-A-Glance.pdf.

[159] Winslow, *supra* note 135, at 84.

on a definition of insurance, may be influenced by factors other than pure insurance theory or economics."[160]

To tell the courts there is no definition or common notion of insurance can correct the tax courts' errors, but it does not provide help to decide if a captive is insurance. Also, there are insurance commissioners and staff who deal with insurance questions every day, and insurers around the world who write trillions of dollars of risk every year. Surely something more can be said as to what is insurance other than: *if it is regulated as insurance then it is insurance*. The *Appleman* test seems the sturdiest of the possible ways to determine what is insurance.[161] Can we build on that? Recognizing the difficulty and possible futility of trying to define insurance beyond risk distribution and risk pooling, perhaps the following provisional definition, informed by the struggles of prior authors, might be considered:

> Insurance is an agreement to provide financial protection against specified categories of future fortuitous losses, by an entity licensed to transact insurance and in the business of insurance, for a specified time, and a specified premium calculable based on anticipated probabilities of individual and aggregate losses that the insurer can likely bear, and on such other terms and conditions agreed upon, and consistent with any regulatory constraints on its operations. The principal object and purpose of this insurance must be solely the transfer of the risk of specified categories of future fortuitous losses, and not be ancillary within any other contract between two parties for the principal purpose of providing goods or services.

This does not solve all the definitional problems or exceptions that can be thought of that perforate even this definition. But this tentative definition, or the *Appleman* test,[162] may work adequately to get a broad enough description that would embrace much of what the insurance domain thinks of as insurance, and thus guide the tax courts in deciding whether particular captive tax cases constitute insurance, even if other factors of the captive relationship are disturbing.

---

[160] *Id.* at 92.
[161] *See supra* note 128.
[162] *Id.*

VI. THE VARIETY OF INSURANCE COMPANIES MAKES FOR UNCOMMON NOTIONS OF INSURANCE

Another factor that affects the tax court decisions of what is insurance, is the idea that insurance must be entirely transferred to another entity. That is largely true. Except the variety of insurance companies means that some risk may be retained by the policyholder itself, beyond the usual deductibles and self-insured retentions. Most insurance companies are stock companies (owned by shareholders) and mutual companies (owned by the policyholders), also called proprietary and cooperative insurers.[163] Similar to a mutual insurer is a reciprocal or interinsurance exchange.[164] These mutuals and their subspecies are important to demonstrate risk distribution among the policyholder-members and to demonstrate that true risk distribution among policyholder-members also involves an element of partial risk retention. As *Couch* explains about these types of insurers:

> A reciprocal or interinsurance exchange is an aggregation of persons, called subscribers, who, through an attorney-in-fact, cooperate to furnish themselves and each other insurance against a designated risk, and the subscribers are both the insured and the insurers. The reciprocal plan is designed for those who desire to assume the positions of both the insurer and the insured for the purpose of eliminating that part of the ordinary insurance premium that goes into profit. Another economy in reciprocal insurance from the standpoint of the subscriber lies in the fact that he or she insures himself or herself at an actual cost without the use of an expensive agency system and also in the lower-loss ratio attributable to the care used in the selection of subscribers.
>
> . . . Again, mutual companies often are incorporated, whereas reciprocal associations or exchanges have no corporate existence, although the attorney-in-fact often does become incorporated.
>
> A reciprocal exchange differs from both stock and mutual insurance companies. It has no stock and no capital as such. The contingent liability of the subscribers to make

---

[163] 3 PLITT, MALDONADO, ROGERS & PLITT, *supra* note 78, § 39:1.
[164] *See id.*

> payments in addition to their premiums stands in the place of the capital of a stock company. The liability of a subscriber is in some respects similar to a liability upon an unpaid subscription to the stock of a corporation.
>
> It appears that a reciprocal or interinsurance exchange is something more than a partnership and something less than an insurance corporation.[165]

Note here the absence of a separate insurance company unrelated to the policyholder, and sometimes even the absence of a separate corporation bearing the insurance (though these associations can be separate legal entities). The reciprocal is more like a partnership, as quoted above, and as Doherty and Dionne explain.[166] This nevertheless is insurance, and is regulated as insurance, because there is risk shifting despite the fact that some risk remains with the insured. Reciprocals were an old form of insurance, before insurance regulation, as explained by a Minnesota court in 1929:

> It is a well-known fact that reciprocal or interinsurance exchanges existed in this country prior to enactment of laws authorizing them. Certain groups of individuals had found this plan an economical and practical method of providing indemnity. One man might not be sufficiently strong financially to bear the risk of loss alone, but he and a number of his friends and acquaintances or others engaged in the same line of business could form a group or association abundantly able to act as their own insurers, and thus procure insurance at or near its actual cost.[167]

Relevant to the current captive insurance taxation question, premiums paid to a reciprocal (for flood insurance) are tax deductible.[168] Thus, risk distribution can exist even when the insured retains a portion of the risk and is exposed to the risk of everyone else. The implication on the

---

[165] *Id.* § 39:48 (citations omitted).

[166] Neil A. Doherty & Georges Dionne, *Insurance with Undiversifiable Risk: Contract Structure and Organizational Form of Insurance Firms*, 6 J. RISK & UNCERTAINTY 187 (1993).

[167] *In re* Minn. Ins. Underwriters, 36 F.2d 371, 372 (D. Minn. 1929).

[168] United States v. Weber Paper Co., 320 F.2d 199, 204–05 (8th Cir. 1963).

captive insurance cases is that total and absolute transfer of the risk (except the deductible) is not a criteria for defining insurance.

Doherty and Dionne, cited in *Ocean Drilling*,[169] provided a definition in that case and also in a prior article where they tried to define insurance. They explained that insurance is often provided by the policyholders themselves in mutual-type companies and pooling arrangements.[170] "[T]here has been a proliferation of new firms such as mutuals, reciprocals, group captive insurance companies, and risk retention groups. The essential feature of all of these organizational forms is that they are owned by their policyholders."[171] This pooling was evident in pollution insurance and earthquake insurance, they wrote.[172] "These organizational structures share the common feature of combining the equityholder and policyholder functions, thereby allocating residual claims on the insurance pool to the policyholders. Risk is pooled amongst those who are commonly exposed rather than transferred to external risk bearers."[173]

A similar consequence is claims-made liability insurance policies that leave the policyholder "exposed to much of the risk of changing liability rules. This is similar in effect to mutualization."[174] The point here is that risk

---

[169] Ocean Drilling & Expl. Co. v. United States, 24 Cl. Ct. 714, 727 (1991), *aff'd*, 988 F.2d 1135 (Fed. Cir. 1993).

[170] Doherty & Dionne, *supra* note 166, at 187–88.

[171] *Id.* at 187.

[172] *Id.* at 187–88.

[173] *Id.* at 187–88. *See also* WILLET, *supra* note 115, at 79–80:

> A member of such a company is not in the same economic situation as one insured for a fixed premium. He has not transferred his risk and purchased security; he has exchanged one risk for another, usually a small chance of a large loss for a larger chance of a smaller loss. Where there is a mere diffusion of loss there remains some degree of uncertainty as to the amount of loss that each member of the group will suffer; where there is complete insurance the insurer has taken upon himself the entire chance of loss, so far as concerns the risks covered by the insurance.

[174] Doherty & Dionne, *supra* note 166, at 188. *See also* Doherty, *supra* note 152, at 228:

> These changes in contract or organizational design have a similar effect. The premium for any given period of cover is random. It is subject to retroactive adjustment on the basis of new information concerning the aggregate loss in the pool. For

transfer can still be in place even when the insurer includes the policyholder as equity holder. Rob Thoyts in *Insurance Theory and Practice* makes a similar point:

> The superficial answer would be that they are transferred to an insurer. The problem with this argument is that recognisable insurance transactions were taking place thousands of years before the first insurance companies appeared. In fact, the risk is being transferred from a number of individuals to a collective pool. This pool contains the collective risk of its members, together with the collective resources these members have set aside to meet the occurrence of such risk. Each member surrenders a small sum to the pool with the intention that this be used to meet the collective loss, regardless of where the loss actually falls.[175]

VII. RISK DISTRIBUTION IS SOMETIMES NOT WIDELY DISTRIBUTED

Risk distribution is not always so clear. One instance is the unique exposures that surplus lines insurers take on. Unlike the standard lines of insurance using the standard measures of pricing and distributing risk through a large number of homogenous exposure units, the surplus lines insurers may not have many homogenous exposure units because, by the nature of risks insured by surplus lines insurers, the risks are unique or unconventional. Nevertheless, these unique risks, while heterogenous, are distributed because they are uncorrelated exposures.

Another instance is small insurers, such as state farm bureau companies, which have concentrated risks, even if they have a decent number of homogenous exposure units. "These mutuals are small, local insurance operations which offer fire insurance primarily on farm property. . . . Some of them operate on an assessment basis which involves a small

---

> example, the mutual may pay a dividend (positive or negative) to its policyholders which is related to the aggregate loss in the pool. The policy holder buying a claims made policy will find that losses which may have arisen, but which have not been presented as claims, within the policy year will be priced in the future in a future insurance contract.

[175] ROB THOYTS, INSURANCE THEORY AND PRACTICE 10–11 (2010).

initial premium but requires the policyholder to pay additional premiums if losses and expenses are greater than anticipated."[176] Distribution cannot be achieved solely within a smaller insurer, because of its narrow geographical range or concentrated lines of insurance or few numbers of insured, yet the insurer is still an insurer and provides important financial protection bearing the risk of its insureds. An example is the Merced Property & Casualty Co. of Atwater, started by farmers in 1906 for fire insurance for a small region of the California Central Valley. [177] After writing 100 insurance policies, it then expanded throughout the region.[178] Then in 2013, being acquired by another insurer, it went insolvent after the Camp Fire wildfire.[179] There were similar exposure units, risk distribution, risk pooling, and yet in a wildfire everything burns, bankrupting the insurer. As a California Court stated, "[w]hether an entity is an insurer does not depend on the entity's size, sophistication, corporate retention policies, or claims handling abilities."[180]

If the idea is that the risk of *this insured* suffering a risk of loss to *this insured's own* property, or liability for *this insured's own* acts, is transferred to another legal entity (minus any retained deductible), then there is no disagreement between the tax courts and insurance law and practice as to risk retention and risk transfer. The real point then of distribution is *pooling,* meaning "the spreading of losses incurred by the few over the entire group, so that in the process, average loss is substituted for actual loss."[181]

---

[176] JAMES L. ATHEARN, RISK AND INSURANCE 385 (1962). *See also* 3 PLITT, MALDONADO, ROGERS & PLITT, *supra* note 78, § 39:17 ("Most of the farm mutuals operate on the unlimited assessment plan, but others may state a definite dollar limitation on the assessment or limit it to a certain multiple of the policyholder's premium."); Annotation, *Liability of Policyholders in Mutual Insurance Companies to Assessments*, 137 A.L.R. 945 (1942). A limited review of the state statutes shows how small these can be. *See, e.g.*, GA CODE ANN. § 33-16-3 (LEXIS through 2021 Reg. Sess.) (only twenty people are needed to start a farm bureau mutual); MINN. STAT. ANN. § 67A.01 (West, Westlaw through 2022 Reg. Sess.) (requiring twenty-five people); TEX. INS. CODE ANN. § 911.053 (West, Westlaw through 2021 Reg. Sess.) (requiring 100 people); COLO. REV. STAT. § 10-12-101 (LEXIS through 2021 Reg. Sess.) (requiring 100 people for a mutual insurance company of any kind).

[177] Dale Kasler & Michael Finch II, *Insurer Goes Bust from Camp Fire with Millions in Claims Unpaid. How Will it Affect Paradise Homeowners?,* SACRAMENTO BEE (Dec. 3, 2018, 12:00 PM), https://www.sacbee.com/news/california/fires/article222563185.html.

[178] *Id.*

[179] *Id.*

[180] Truck Ins. Exch. v. Amoco Corp. 41 Cal. Rptr. 2d 551, 556 (Cal. Ct. App. 1995).

[181] REJDA & MCNAMARA, *supra* note 110, at 20.

"[B]y pooling, or combining the loss experience of a large number of exposure units, an insurer may be able to predict future losses with greater accuracy."[182]

Insurers, big and small, solve the problem of inadequate risk distribution by buying reinsurance. The total premiums spent on reinsurance in 2019 were $61.8 billion dollars for the top twenty-five reinsurers:[183] "Basically, reinsurance is a mechanism for spreading risk."[184] Distribution is therefore achieved vertically, through reinsurance.[185] "[W]here an insurer is unwilling to assume at its own risk the whole of the insurance offered, it nevertheless does so, and reinsures so much of it in such form as it deems suitable and necessary to reduce its own ultimate exposure to loss to proper limits."[186] Insurers need the operational capacity of reinsurers "to sustain and survive catastrophic losses, the capacity to achieve statistically predictable loss behaviour, the capacity to carry costs of acquiring larger and larger amounts of new insurance . . . ."[187] In this way, the "gross underwriting capacity of the reinsurer may be said to have added to that of the ceding [primary] insurer . . . . The underwriting capacity of the reinsurer becomes the channel through which more even distribution of risk is achieved for the insurer."[188]

---

[182] *Id.* at 21. *See also* FRANK H. KNIGHT, RISK, UNCERTAINTY AND PROFIT 232–35 (1921). This goes back to the spread of risk, and the law of large numbers to forecast expected losses and thus to price the risk. Knight's point is expanded upon in George L. Head, *An Alternative to Defining Risk as Uncertainty*, 34 J. RISK & INS. 205 (1967). The debate about the meaning of risk is as broad as the debate about the meaning of insurance, and depends on the discipline doing the defining and the context.

[183] REINSURANCE ASS'N OF AM., REINSURANCE UNDERWRITING REVIEW: A FINANCIAL REVIEW OF U.S. REINSURERS 2019 INDUSTRY RESULTS 1 (2020), https://www.reinsurance.org/RAA/Industry_Data_Center/Reinsurance_Underwriting_Review/Reinsurance_Underwriting_Review.html.

[184] STEVEN C. SCHWARTZ, REINSURANCE LAW: AN ANALYTIC APPROACH § 2.02 (2018).

[185] *See* 1 STARING & HANSELL, *supra* note 20, § 1:3; Henry T. Kramer, *The Nature of Reinsurance*, *in* REINSURANCE 1, 6 (Robert W. Strain ed., 1980).

[186] Kramer, *supra* note 185, at 6. *See also* Thimann, *supra* note 138, at 6 ("The managing of risk takes place through pooling or mutualization— that is, the aggregation of a large number of similar risks, . . . or it takes place through cession [to reinsurers] and diversification . . . .").

[187] Kramer, *supra* note 185, at 3.

[188] *Id.* at 28.

> The control of an insurer's severity of loss by reinsurance is less a matter of theory or convenience than a necessity. . . . As a practical marketing matter, most insurers are obliged to accept sums insured which exceed the net retained limits within which the law of large numbers will work, at least over periods as short as one year or less. Viewed this way, reinsurance is a commercial activity that permits an insurer to do what it wants: to issue policies in the amounts required by its insureds.[189]

It has been stated that "'captive' insurance companies provide a testimonial to the necessity of reinsurance and its ability to provide capacity."[190] As the author explained in 1980, "without the availability of reinsurance one of the most interesting developments in the insurance business [captives] in the last twenty years would never have occurred."[191] The older *Appleman* treatise explained the importance of reinsurance to self-insured entities, which would include captives:

> Reinsurance is important to a self insurance program for a number of reasons. These reasons are quite similar to the functions played by reinsurance in the broader insurance market. First, it enables the program to establish a ceiling on the risks it will retain. Second, it enables the program to write risks it would otherwise deem unattractive, because of the ability of the program to share the risk through reinsurance. Third, it enables the program to obtain larger limits than if the program utilized solely its own internal capital and premiums. Finally, it enables the capital of the program to be used to write larger risks.[192]

Thus, the notion of risk distribution must be adjusted to the reality that insurers often do not achieve sufficient distribution in their portfolio,

---

[189] *Id.* at 29. *See also* SCHWARTZ, *supra* note 184, § 2.02[3] ("By laying off part of the risk to its reinsurers, a company can write a policy that, without reinsurance, would have been beyond its underwriting capacity. Similarly, reinsurance may enable a company to write a greater number of policies, with a larger aggregate exposure, than it could without reinsurance.").

[190] Robert A. Baker, *The Purpose of Reinsurance*, *in* REINSURANCE 33, 34 (Robert W. Strain ed., 1980).

[191] *Id.*

[192] 14 HOLMES, *supra* note 87, § 102.7.

either because of an insufficient number of exposure units or limited geographical dispersion that subjects the units to the possibility of a common peril. To achieve practical, prudent, and profitable distribution, insurers, therefore, use reinsurance.

Sometimes risk is not entirely shifted away from the insured at all because the insurance is more of a mutual aid or pooling arrangement (disregarding deductibles and self-insured retentions). This is particularly so with risk retention groups, "whose primary activity consists of assuming and spreading all, or any portion, of the liability exposure of its group members," as authorized under the Federal Liability Risk Retention Act of 1986,[193] and which are "chartered or licensed as a liability insurance company under the laws of a State and authorized to engage in the business of insurance under the laws of such State . . . ."[194] Such risk retention groups are owned by the members.[195]

Further examination can be made of the fraternal organizations[196] and assessment mutual companies[197] to the same result. Insureds buy

---

[193] Risk Retention Act of 1986, 15 U.S.C. § 3901(a)(4)(A).

[194] § 3901(a)(4)(C)(i). For statutory examples, see N.Y. INS. LAW § 5902 (McKinney, Westlaw through 2022 Legis.); CONN. GEN. STAT. § 38a-250 (West, Westlaw through 2022 Reg. Sess.).

[195] § 3901(a)(4)(E).

[196] *See, e.g.*, Nicholas F. Potter, *Fraternal Benefits Societies, in* 4 NEW APPLEMAN NEW YORK INSURANCE LAW § 51.05 (Wolcott B. Dunham & Aviva Abramovsky eds., 2d. ed., LEXIS, database updated Nov. 2021):

> Fraternal benefit societies are unique in their corporate structure, purposes and functions. They were primarily organized by groups of immigrants and their descendants. Their purpose was to provide a vehicle through which persons of common ethnic, national, or religious backgrounds, and workers in a common hazardous occupation or craft, could join together in local lodges to promote and retain their heritage and customs while at the same time provide a modicum of insurance protection for their members and families.

[197] *See, e.g.*, Md. Motor Truck Ass'n Workers' Comp. Self-Ins. Grp. v. Prop. & Cas. Ins. Guar. Corp., 871 A.2d 590, 598 (Md. 2005):

> The mere fact that the members retain joint and several liability for any remaining obligations of the Group does not suffice to preclude the Agreement from constituting an insurance contract. Section 504 of the Agreement also provides for the

insurance to transfer substantial risk, but they retain the risk of deficiencies if the insurer has insufficient surplus to pay for the losses, thus retaining some risk beyond their own deductibles. Despite this incomplete risk transfer, fraternal organizations and assessment mutual companies constitute insurance for state insurance purposes.[198]

Winslow, reviewing the insurance economics literature, contends that distribution can be difficult to define and may not even be necessary.[199] Further, an insured with a large number of exposure units—let's say a retail store with hundreds or thousands of locations, or a firm with a fleet of vehicles—may have enough frequency of losses that the uncertainty of loss becomes fairly certain. Once that happens, the purpose of insurance (to insure against uncertainty) disappears, thus defeating a captive insurance arrangement on the very grounds by which it is supposed to exist, by insuring a large number of exposure units.[200] We need not debate or resolve that here.

All these examples show that insurance exists perfectly well even when the insured shares in the risk of others and does not absolutely transfer the entire risk to another risk-bearing entity as a modern (but not necessarily traditional) insurer. Courts and insurance regulators have neither rejected risk groups nor small assessment mutuals on the grounds of tax courts' notions of insurance and inadequate distribution of risk. It might be more accurate to say that the traditional insurer was an association of insureds, and later an association of insurers in a reciprocal exchange of reinsurance, resulting in a better "spread of risk."[201]

CONCLUSION

Defining insurance beyond the core is hard even within the insurance domain. Insurance involves risk shifting and indemnity, and more than that, because that can be done in any contract between parties as ancillary to a

---

> distribution of surplus funds, not needed for the payment of claims and administrative expenses or for a prudent cushion, to the members in the form of dividends. Such an arrangement—joint and several liability for a deficiency and the right to recover part of the surplus funds in the form of dividends—is a traditional characteristic of assessment mutual insurance companies.

[198] *See supra* notes 196–97.

[199] Winslow, *supra* note 135, at 150–58.

[200] *Id.* at 160–61. *See also* WILLET, *supra* note 115, at 4-8 (discussing the distinction between probability and uncertainty when defining risk).

[201] Kramer, *supra* note 185, at 2.

contract for goods and services. Risk transfer must be the primary goal of the contract. That involves risk distribution, which is often horizontal distribution among similar units, and sometimes among non-similar units if they are not correlated, as is done with unique risks in the surplus lines market. It is also done with vertical distribution through reinsurance where the insurer is too small to absorb a large individual loss or a large aggregate loss. The *Appleman* test of looking at the object and purpose of the transaction[202] is probably the best characterization of insurance, and the insurance definition offered within this article might also serve to embody the insurance industry's and insurance regulator's practice and consensus of what is insurance.

The tax courts' factors for determining insurance "in the commonly accepted sense" are mostly irrelevant to determining insurance, though they are important to trying to understand whether there are tax games afoot that try to hide behind insurance. The "resolution [whether a captive insurance arrangement is proper for tax purposes] lies not with the definition of insurance, but with the policies behind general tax doctrines, such as protection of federal tax revenues, promotion of certainty in tax planning, and encouragement of legitimate business transactions."[203] Tax judgment is required to ascertain those situations, but tax judgment about what is insurance should defer to the insurance domain to ascertain insurance situations because insurance can go far beyond what tax practitioners may think are core "commonly accepted" notions to insurance and insurable risks.

---

[202] *See supra* note 128.

[203] Winslow, *supra* note 135, at 112 (citations omitted).

THE CASE FOR BANNING (AND MANDATING) RANSOMWARE INSURANCE

KYLE D. LOGUE* & ADAM B. SHNIDERMAN**

ABSTRACT

Ransomware attacks are becoming increasingly pervasive and disruptive, resulting in ransom demands becoming more exorbitant. Payments for ransom costs are increasingly being covered by insurance, which may offer coverage for a variety of cyber-related losses. Some commentators have expressed concern over this market phenomenon. Specifically, the concern is that the presence of insurance is making the ransomware problem worse based on the following theory: because there is ransomware insurance that covers ransom payments, and because paying the ransom is often far cheaper than paying the restoration and business interruption costs covered under the policy, there is an increased tendency to pay the ransom—and a willingness to pay higher amounts. This fact, known by the criminals, increases their incentive to engage in ransomware attacks, which increases the demand for insurance. And the cycle continues.

This Article demonstrates that the picture is not as simple as this story would suggest. Insurance offers a variety of pre-breach and post-breach services that are aimed at reducing the likelihood and severity of a ransomware attack. Thus, over the long-term, cyber insurance has the potential to lower ransomware-related costs, even without government intervention. As recent research has shown, however, insurers have not yet fully embraced their potential role as ex ante and ex post regulators of cyber risk—a role for which they are especially well-suited. This Article discusses reasons why that might be the case and offers suggestions for how government intervention may help. Among these suggestions is a limited ban on indemnity for ransomware payments with exceptions for cases involving threats to life and limb, which would be an expanded version of what is already in place with the Office of Foreign Assets Control's ("OFAC") sanctions program. We also explain how a government regulator, such as

---

* Douglas A. Kahn Collegiate Professor of Law, University of Michigan Law School.

** Law Clerk, U.S. Court of Appeals for the Ninth Circuit. The views expressed herein are the authors' own and are not intended to reflect the views of their employers. The authors appreciate the helpful suggestions of Asaf Lubin, Daniel Schwarcz, Peter Siegelman, and Jeffrey Thomas, as well as the other participants in the New Ideas in Insurance program at the Insurance Law Center at the University of Connecticut School of Law.

the OFAC, could serve a coordinating function to help cyber insurers internalize the externalities associated with the insurers' decisions to reimburse ransomware payments—a role that is played by reinsurers in the context of kidnap-and-ransom insurance. Finally, we consider the idea of a federal mandate requiring property and casualty insurers to provide coverage for the costs of ransomware attacks but exclude coverage for the ransomware payments.

TABLE OF CONTENTS

INTRODUCTION

Ransomware attacks are increasingly pervasive and disruptive. Not only are they shutting down (or at least "holding up") businesses and local governments across the country, they are disrupting institutions in many sectors of the U.S. economy—from school systems, to medical facilities, to critical elements of the U.S. energy infrastructure, as well as the food supply

chain.[1] In one recent example that grabbed the world's attention, a ransomware attack halted fuel distribution at Colonial Pipeline, which supplies roughly forty-five percent of the diesel, gasoline, and jet fuel used on the East Coast.[2] Ransomware attacks are also growing more frequent and the ransom demands more exorbitant.[3] Indeed, the attacks are getting more pernicious with every passing month.[4] What's more, as Commerce Secretary Gina Raimondo has noted, ransomware attacks "are here to stay."[5]

---

[1] Heather Kelly, *Ransomware Attacks Are Closing Schools, Delaying Chemotherapy and Derailing Everyday Life*, WASH. POST (June 5, 2021, 8:00 AM), https://www.washingtonpost.com/technology/2021/07/08/ransomware-human-impact/ (describing increasing prevalence and seriousness of ransomware attacks). Among the recent targets have been the Baltimore school system, a meat processing company, and the ferry system at Martha's Vineyard. *Id.*

[2] *See id.*; Lily Hay Newman, *Colonial Pipeline Paid a $5M Ransom—And Kept a Vicious Cycle Turning*, WIRED (May 14, 2021, 7:00 AM), https://www.wired.com/story/colonial-pipeline-ransomware-payment/; David E. Sanger, Clifford Krauss & Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html. According to the Congressional testimony of Colonial's CEO, the hackers were able to exploit Colonial Pipeline's failure to use dual authentication technology in its network. *See* Stephanie Kelly & Jessica Resnick-Ault, *Hackers Only Needed a Single Password to Disrupt Colonial Pipeline, CEO Testifies*, INS. J. (June 9, 2021), https://www.insurancejournal.com/news/national/2021/06/09/617870.htm. The Colonial Pipeline attack prompted one U.S. Congressman to call ransomware "an existential threat" to the country's energy system. Celine Castronuovo, *Ron Johnson Calls Cyber Attacks an 'Existential' Threat Following Colonial Pipeline Shutdown*, THE HILL (May 16, 2021, 7:00 AM), https://thehill.com/homenews/sunday-talk-shows/553725-ron-johnson-calls-cyber-attacks-an-existential-threat-following?rl=1.

[3] Suzanne Barlyn, *Global Insurers Face Quiet Strain from Hacker Ransom Demands*, REUTERS (Oct. 25, 2019, 7:20 AM), https://www.reuters.com/article/us-usa-ransomware-insurance/global-insurers-face-quiet-strain-from-hacker-ransom-demands-idUSKBN1X41E3. *See infra* Part II.

[4] *See Ransomware Attack Vectors Shift As New Software Vulnerability Exploits Abound*, COVEWARE (Apr. 26, 2021), https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound (noting the increase in ransom payments by quarter).

[5] David Cohen, *Ransomware Attacks 'Are Here to Stay,' Commerce Secretary Says*, POLITICO (June 6, 2021, 10:28 AM), https://www.politico.com/news/2021/06/06/ransomware-attacks-commerce-secretary-492005.

For those who have not been following this alarming development, ransomware is a type of malicious software ("malware") that suspends a computer system's backup functions, encrypts the user's files, and demands a ransom payment in exchange for the unlock key.[6] Much like other computer viruses, ransomware can enter a user's system through several paths, including user error (e.g., when an employee clicks a malicious link received in an email message) or vulnerabilities in the network itself.[7] Once a computer or network is infected, the user is faced with choosing either to rebuild the system or pay the ransom.[8] Due to the high cost of rebuilding computer networks, organizations that have fallen victim to ransomware attacks (including hospitals, schools, businesses, and municipalities) have become more inclined to simply pay the ransom.[9]

In a trend that some find disturbing, ransom payments are increasingly being covered by insurance.[10] Just as it is possible to buy insurance coverage against the risk of being kidnapped for ransom,[11] it is

---

[6] *Ransomware*, FED. BUREAU OF INVESTIGATION: SCAMS & SAFETY, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (last visited Mar. 31, 2022).

[7] *Id.*

[8] *Id.*

[9] Newman, *supra* note 2 ("[I]n practice many organizations resort to paying. They either don't have the backups and other infrastructure necessary to recover otherwise, can't or don't want to take the time to recover on their own, or decide that it's cheaper to just quietly pay the ransom and move on."). Colonial Pipeline, for example, paid DarkSide, the Russian criminal cyber cartel responsible for most recent attack, a seventy-five bitcoins ransom worth approximately $5 million at the time. *Id.* The Department of Justice subsequently recovered sixty-four of those bitcoins, worth roughly $2.3 million. MacKenzie Sigalos, *The FBI Likely Exploited Sloppy Password Storage to Seize Colonial Pipeline Bitcoin Ransom*, CNBC (June 9, 2021, 7:09 AM), https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html. Ironically, the DOJ apparently was able to exploit the hackers' sloppy use of passwords in securing their bitcoin wallet. *Id.*

[10] *See* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00 AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks. As of the time this Article, it remains unclear whether Colonial Pipeline relied on an insurer or simply paid the ransom out of its own coffers.

[11] *See generally* ANJA SHORTLAND, KIDNAP: INSIDE THE RANSOM BUSINESS (2019).

also possible to buy insurance against the risk of a ransomware attack. As a result of the growing number of cyber threats and the insurance market's response to increasing demand for coverage, the market for specialized cyber insurance policies has expanded dramatically in recent years.[12] Such policies offer coverage for a variety of cyber-related losses, including many of the costs arising out of ransomware attacks, such as the costs of hiring expert negotiators, the costs of recovering data from backups, the legal liabilities for exposing sensitive customer information, and the ransom payments themselves.[13] Perhaps unsurprisingly, then, parties with ransomware insurance are increasingly relying on their insurance carrier to negotiate ransom demands and indemnify the payments.[14]

Some commentators have expressed concern with this market phenomenon. Specifically, there is concern that the presence of insurance is making the ransomware problem worse.[15] Arguably, the most extreme

---

[12] *See* Dudley, *supra* note 10 ("In recent years, cyber insurance sold by domestic and foreign companies has grown into an estimated $7 billion to $8 billion-a-year market in the U.S. alone . . . ."). *See also infra* Part III (describing the structures of a cyber insurance policy and its ransomware coverage).

[13] *See, e.g.*, Barlyn, *supra* note 3 (discussing nature of trends in ransomware attacks and nature of coverage). A number of insurers now provide coverage for many of the costs of ransomware attacks in their standalone cyber insurance policies. *See, e.g.*, AIG INC., CYBEREDGE WORDING SAMPLE SPECIMEN FORM (2021), https://perma.cc/T3VD-JR8R; X.L. AM., INC., CYBERRISKCONNECT: PRIVACY, SECURITY AND TECHNOLOGY INSURANCE (2019), https://axaxl.com/-/media/axaxl/files/pdfs/insurance/cyber-north-america/cyberriskconnectpolicyform_axaxl_trd-050-0619.pdf?sc_lang=en&hash=8E1AC2226AA2330E5A9276F3A49E332F. Some insurers also provide somewhat overlapping coverage in their kidnap & ransom policies. *See, e.g.*, AM. INT'L GRP., INC., CYBER COVER GUIDE (2018), https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-cover-grid.pdf [hereinafter AIG CYBER COVER GUIDE].

[14] *See* Dudley, *supra* note 10.

[15] *See* Alex Scroxton, *Is It Time to Ban Ransomware Insurance Payments?*, COMPUTERWEEKLY.COM (Feb. 11, 2021), https://www.computerweekly.com/feature/Is-it-time-to-ban-ransomware-insurance-payments (quoting Erin Kenneally, director of cyber risk analytics at Guidewire and former staffer in the U.S. Department of Homeland Security's cyber division, saying "insurers have taken a rational economics approach to ransomware payments, leading to a growing sentiment that the industry is worsening the problem by paying extortions."); Zoe Kleinman, *Insurers Defend Covering Ransomware Payments*, BBC: NEWS (Jan. 27, 2021), https://www.bbc.com/news/technology-55811165; Danny Palmer,

version of this claim appeared in an August 2019 *ProPublica* story that linked the rise of ransomware attacks with the presence of cyber insurance.[16] Noting several examples of insurance companies paying ransom demands to unlock their insured's systems, the *ProPublica* author suggests that the insurance industry has contributed to a vicious cycle that fuels ransomware attacks while padding insurers' bottom lines.[17] And the author gave this collection of phenomena the evocative label, "the extortion economy."[18] The logic behind this label goes something like the following: once an insurer has sold a cyber insurance policy to an insured (e.g., a city or a corporation), that insurer has a strong incentive to pay any ransom that is demanded. Paying the ransom, though costly, may be much cheaper than paying the restoration costs that will be incurred if the ransomware program is not "unlocked" by the hacker.[19] These restoration costs, under the terms of the typical cyber policy, will be borne by the insurer rather than the insured.[20] Thus, a simple cost-benefit analysis will, on this view, inevitably lead the insurer to prefer paying the ransom. Hackers understand this logic, which gives them a strong incentive to identify and attack organizations that have cyber insurance coverage.[21] This dynamic leads to more hacking and ransomware attacks overall, which increases demand for cyber insurance. As a result, insurers can sell more policies for higher premiums than before. And the cycle continues. The (mostly implied) conclusion of such analyses is that

---

Ransomware: Cyber-Insurance Payouts Are Adding to the Problem, Warn Security Experts, ZDNET (Sept. 17, 2019), https://www.zdnet.com/article/ransomware-cyber-insurance-payouts-are-adding-to-the-problem-warn-security-experts/.

[16] Dudley, *supra* note 10. *See also* Victoria Hudgins, *Rising Ransomware Attacks Spur Debate over Whether Cyber Insurance Is to Blame*, LAW.COM: LEGALTECH NEWS (Dec. 4, 2020, 9:00 AM), https://www.law.com/legaltechnews/2020/12/04/rising-ransomware-attacks-spur-debate-over-whether-cyber-insurance-is-to-blame/?slreturn=20201110104215; Palmer, *supra* note 15.

[17] Dudley, *supra* note 10.

[18] *Id.*

[19] *Id.* (discussing multiple circumstances where it was cheaper to pay ransom).

[20] *See infra* Part III (describing the structures of a cyber insurance policy and its ransomware coverage).

[21] Indeed, it appears hackers are threatening to act on the incentive. *See* Chris Beck & Blake Fleisher, *Does It Ever Make Sense for Firms to Pay Ransomware Criminals?*, INS. J. (July 8, 2021), https://www.insurancejournal.com/news/international/2021/07/08/620508.htm; Hudgins, *supra* note 16.

we would be better off if the market for ransomware insurance were to disappear.[22]

This claim has gained traction in the popular media, government officials, members of the legal profession, and commentators in academia. The former head of the U.K.'s National Cyber Security Center, Ciaran Martin, for example, recently asserted that the ransomware problem is being fueled by the absence of legal barriers to organizations paying ransoms and filing insurance claims.[23] Martin went on to suggest the possibility of an outright ban on insurance coverage for ransomware payments.[24] The U.S. Department of the Treasury, through the OFAC, issued an advisory highlighting existing federal law that authorizes steep fines on U.S. persons, individuals and entities who make payments to parties under sanction by the U.S. government.[25] The narrative that ransomware insurance makes businesses a target has been embraced by privacy and data security lawyers as well. As one attorney put it, a reason hackers target small to medium-sized companies and municipalities, which probably do not have large amounts of cash in the bank for paying ransom demands, is that such entities are likely to have insurance coverage.[26]

This idea—that the presence of insurance coverage actually encourages ransomware attacks—is an example of a more general phenomenon recently identified by two legal scholars as the problem of

---

[22] There is some possibility that this could happen. One large cyber insurer, AXA, which had been providing ransomware coverage, has—at the request of French government officials—decided to stop selling cyber insurance in France that reimburses extortion payments to ransomware criminals. Frank Bajak, *Insurer AXA to Stop Paying Ransomware Crime Payments in France*, INS. J. (May 9, 2021), https://www.insurancejournal.com/news/international/2021/05/09/613255.htm.

[23] Dan Sabbagh, *Insurers 'Funding Organised Crime' by Paying Ransomware Claims*, GUARDIAN (Jan. 24, 2021), https://www.theguardian.com/technology/2021/jan/24/insurers-funding-organised-by-paying-ransomware-claims.

[24] *Id.*

[25] U.S. Dep't of the Treasury's Off. of Foreign Assets Control, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [hereinafter U.S. Dep't of the Treasury's Advisory]. *See infra* notes 232–45 and accompanying text.

[26] Hudgins, *supra* note 16 (quoting Philip Yannella, privacy and data security group practice leader at Ballard Spahr).

"third-party moral hazard."[27] In a paper entitled *The Paradox of Insurance*, Gideon Parchomovsky and Peter Siegelman explore the potential for insurance to create significant negative externalities through incentives for third parties—that is, parties other than the insureds or the insurers—to "engage in antisocial, illegal and unethical activities in order to extract money from insureds or insurers."[28] The basic idea is straightforward and persuasive. If a third-party is interested in extorting or defrauding (or, in any way, illegally extracting) money from another individual or organization, the fact that the target individual or organization has insurance for such a payment can increase the third-party's incentives to undertake such a scheme and can influence how much money they try to extract.[29] The more money is available to pay an extortion demand, all else equal, the more profitable the extortion demand can be. Although Parchomovsky and Siegelman do not address ransomware insurance specifically, they do address kidnap-and-ransom ("K&R") insurance, which has obvious similarities with ransomware coverage.[30]

What should be done about the third-party moral hazard effects of ransomware insurance? One suggested solution is to ban such coverage, either as general ban on making ransom payments or as a narrower ban on the insurance industry from selling coverage for such payments.[31] The

---

[27] Gideon Parchomovsky & Peter Siegelman, *The Paradox of Insurance* (Univ. of Penn. Inst. for L. & Econ., Research Paper No. 20-20), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3160&context=faculty_scholarship.

[28] *Id.* at 2.

[29] *Id.* at 4, 9–10.

[30] *Id.* at 6 ("But perhaps the case that best illustrates the paradox of insurance is kidnap insurance."). In a footnote to this statement, they then acknowledge that "kidnap insurance has evolved various techniques to mitigate third party moral hazard." *Id.* at n.7 (citing Anja Shortland, *Governing Kidnap for Ransom: Lloyd's as a "Private Regime"*, 30 GOVERNANCE 283 (2017)). Parchomovsky and Siegelman also cite to other recent works on kidnapping and insurance. *See, e.g.*, Alexander Fink & Mark Pingle, *Kidnap Insurance and Its Impact on Kidnapping Outcomes*, 160 PUB. CHOICE 481 (2014). We discuss the work of Parchomovsky and Siegleman as well as the work of Anja Shortland and their relevance to the ransomware insurance case below. *See infra* Part III & Part IV.B.1.

[31] One threat analyst has claimed that "[p]rohibiting ransomware payments is the quickest and most effective way to end ransomware attacks." Jason Breslow, *How to Stop Ransomware Attacks? 1 Proposal Would Prohibit Victims from Paying Up*, NPR (May 13, 2021, 12:03 PM), https://www.npr.org/2021/05/13/996299367/how-to-stop-ransomware-attacks-1-proposal-would-prohibit-victims-from-paying-

reasoning for such a ban is simple and compelling. If ransom payments, or the insurance for ransom payments, were to be prohibited by law (e.g., under penalty of heavy fines), the likelihood that a ransomware victim would actually make the ransom payment would decrease. And if ransomware targets are less likely to pay, or the amounts they are willing to pay are diminished (because of the lack of insurance funds as a potential source of financing), the hackers' incentive to demand a ransom would also be diminished. This reasoning not only serves as the basis for recent calls to enact bans on ransomware payments and ransomware insurance, it has for many years also served as the basis for calls to ban ransom payments and ransom insurance in the kidnapping setting.[32]

Assuming that the primary motivation for most ransomware attacks is financial, as seems to be the case (at least for now),[33] this argument has some obvious merit. However, it fails to take into account the practical and moral limitations that would be raised by a comprehensive ban on ransomware payments and insurance coverage.[34] Given the explosion in the

---

up (quoting Brett Callow, threat analyst with Emsisoft). *See also* Emer Scully, *Ex GCHQ Boss Calls for Ban on Ransom Payments to Hackers After Criminals Targeted Hospitals in Ireland and Largest Pipeline in US Closed Due to Cyber Attack*, DAILYMAIL (May 15, 2021), https://www.dailymail.co.uk/news/article-9581635/Ex-GCHQ-boss-calls-ban-ransom-payments-criminals-targeted-hospitals-Ireland.html; Phil Goldstein, *New York May Ban Ransomware Payments from Municipalities*, STATETECH MAG. (Mar. 9, 2020), https://statetechmagazine.com/article/2020/03/new-york-may-ban-ransomware-payments-municipalities.

[32] *See, e.g.*, Yvonne M. Dutton & Jon Bellish, *Refusing to Negotiate: Analyzing the Legality and Practicality of a Piracy Ransom Ban*, 47 CORNELL INT'L. L.J. 299 (2014).

[33] Most of the reporting on the rise of ransomware attacks indicates that profit is the primary motive. *See, e.g.*, Alexander S. Gillis & Ben Lutkevich, *Definition: Ransomware*, TECHTARGET, https://www.techtarget.com/searchsecurity/definition/ransomware (last updated Dec. 2021). To the extent ransomware attacks are not about profit-maximization for the attackers, but rather are part of either a terrorist plot or cyber hybrid warfare effort on the part of a nation to another nation's economy (as was the case for the massive NotPetya attack), it is not clear that the extortion economy story would apply in the same way, and it is therefore not clear that the same responses would be called for. For discussion on the NotPetya attack, see *infra* notes 50–53 and accompanying text.

[34] So far as we are aware, the U.S. government has never enforced a ban on a particular type of insurance categorically. As we discuss below, however, there is a statutory ban on payments to individuals and organizations subject to U.S. sanctions,

sheer number of ransomware attacks in recent years,[35] enforcing a universal ban on all ransomware payouts by individual victims would be impractical. It would be a daunting administrative undertaking for the government to monitor thousands, perhaps tens of thousands, of organizations and individuals to ensure compliance with a comprehensive ransom ban, especially given the difficulty of tracking cryptocurrency transactions.[36] In addition, if bans on ransomware insurance ended up curtailing all insurance coverage for ransomware attacks, we would lose all of the potential regulatory benefits that insurance can provide. Put another way, when insurance companies provide coverage for a particular risk, they have incentives in competing for business to help their insureds find methods to minimize their risks.[37] Banning insurance in this part of the cyber risk market would eliminate that potential regulatory benefit that insurance provides, in

---

which ban on its face does seem to apply to ransom payments by insurers. Whether that ban is enforced is another matter. *See infra* Part IV.B.

[35] There have been thousands of ransomware attacks reported in recent years. The FBI's Internet Crime Complaint Center ("IC3") asserts there were 2,474 ransomware incidents reported in 2020 and a 225 percent increase in ransom demands. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, AA21-243A, NATIONAL CYBER AWARENESS SYSTEM ALERT: RANSOMWARE AWARENESS FOR HOLIDAYS AND WEEKENDS 2 (2022), https://www.cisa.gov/uscert/sites/default/files/publications/AA21-243A-Ransomware_Awareness_for_Holidays_and_Weekends.pdf. Then IC3 received 2,084 complaints in the first half of 2021. *Id.* Several times that number goes unreported. Gerrit De Vynck, *Many Ransomware Attacks Go Unreported. The FBI and Congress Want to Change That*, WASH. POST (July 27, 2021, 7:32 PM), https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-ransomware-laws/ (quoting Eric Goldstein, executive assistant director at CISA, as saying, "[w]e believe that only about a quarter of ransomware intrusions are actually reported.").

[36] *See infra* notes 99–110 and accompanying text.

[37] For a discussion of the ways in which various types of insurance seek to reduce insured's losses, see KENNETH S. ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY 57 (1986); RICHARD V. ERICSON, AARON DOYLE & DEAN BARRY, INSURANCE AS GOVERNANCE (2003); Tom Baker & Thomas O. Farrish, *Liability Insurance & the Regulation of Firearms*, *in* SUING THE GUN INDUSTRY: A BATTLE AT THE CROSSROADS OF GUN CONTROL AND MASS TORTS 292 (Timothy D. Lytton ed., 2005); and Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012). We discuss insurance as a source of cyber risk regulation further below. *See infra* Part IV.B.

addition to the obvious risk-spreading benefit. What's more, a ban on ransomware payments and ransomware insurance raises moral and practical concerns. Would the ban require imposing a serious punishment on, say, a hospital administrator who decides to pay a ransomware demand rather than risk the lives of its patients, or on the insurer who facilitates that payment?

On the other hand, even if one were to conclude that ransomware insurance should not be banned in all circumstances, such a conclusion would not imply that all government intervention in the ransomware insurance market is a bad idea. For starters, any insurance contract that covers ransomware attacks should be subject to the same sorts of regulatory safeguards and common-law doctrines that govern other aspects of the insurance relationship between insurers and their policyholders.[38] Further, the potential regulatory or governance function of insurance has natural limitations. For example, ransomware insurers themselves externalize some of the costs of ransomware attacks, which means that their incentives as regulators will not be optimal, which provides additional potential roles for government intervention.[39]

For these reasons, this Article considers a different approach, primarily as a thought experiment. First, to interrupt the extortion economy described above, we could institute a federal ban on insurance coverage for ransomware payments. This ban would apply to all insurance payouts for

---

[38] The insurance industry is regulated at the state level. The seven main functional types of state insurance regulation include "(1) licensing (of insurance companies and intermediaries), (2) taxation, (3) solvency, (4) rates, (5) forms, (6) access and availability, and (7) market conduct." TOM BAKER, KYLE D. LOGUE, & CHAIM SAIMAN, INSURANCE LAW AND POLICY: CASES AND MATERIALS 142 (5th ed. 2021). In addition, insurance contracts are subject to the same sorts of interpretive principles and common law doctrines that apply to other contracts and that serve to protect the reasonable expectations of the insureds and the insurers. Such doctrines include contra proferentem, waiver and estoppel, misrepresentation, and the duty of good faith and fair dealing. *See id.* at ch.2. *See also infra* Part II.C.

[39] As Shortland points out, in the kidnap-and-ransom insurance market, the reinsurer Lloyd's of London helps to internalize these externalities by serving a sort of industry coordinating function. SHORTLAND, *supra* note 11, at 176–77. *See also* Parchomovsky & Siegelman, *supra* note 27, at 34–35 (noting Shortland's conclusion regarding the beneficial coordination role that Lloyd's plays int the K&R market). We discuss below why reinsurers are less likely to play such a coordinating role in the ransomware insurance market and thus why government intervention may be necessary. *See infra* Part IV.B.1.

ransom payments except in situations involving substantial threat to human health or life. Second, with respect to coverage for the other losses associated with ransomware attacks (including the costs of restoring victims' computer networks as well as business interruption coverage), not only would there be no ban, there would be a mandate that all commercial property and casualty insurers offer such coverage in a standalone policy that contains a reasonable amount of coverage—that is, with policy limits that provide substantial coverage in the event of an attack. Third, to encourage the purchase of such coverage, lawmakers could enact some sort of federal subsidy for the purchase of cyber insurance. The most obvious candidate would be an insurer-side subsidy in the form of a federal backstop or reinsurance program, similar to the sort of program that is already in place for terrorism insurance.[40] But if such a program did not prove to be a sufficient subsidy and not enough organizations end up purchasing cyber insurance coverage, there are other, more extreme (less politically plausible, but perhaps more interesting), options such as a buyer-side subsidy or even a mandate. This would be similar to compulsory auto liability insurance or healthcare coverage under the Affordable Care Act.[41]

This Article unfolds as follows. Part II provides a brief overview of the phenomenon of ransomware attacks—how they evolved from prior generations of cyberattacks, what forms the attacks tend to take now, and how the hackers secure their ransom. Part III considers the development of cyber insurance, with a special emphasis on coverage for ransomware attacks and how ransom negotiations are carried out in the shadow of the existing contractual obligation represented in the cyber insurance policy. Part III describes the structure of the ransomware insurance contract, and how the dynamics in the ransomware coverage market and the doctrines of insurance

---

[40] *See* Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322 (2002). *See infra* Part IV.B.1.

[41] Every state has some form of automobile financial responsibility law, which typically requires some minimal level of auto liability insurance coverage. *See Vehicle Liability Insurance Requirements*, U.S. DEP'T OF STATE, https://www.state.gov/vehicle-liability-insurance-requirements/ (last visited Apr. 1, 2022). *See generally Automobile Financial Responsibility Laws by State*, INS. INFO. INST., https://www.iii.org/automobile-financial-responsibility-laws-by-state (last updated July 2018). The Affordable Care Act originally required most people to purchase health insurance. CHRISTINE EIBNER & SARAH A. NOWAK, THE EFFECT OF ELIMINATING THE INDIVIDUAL MANDATE PENALTY AND THE ROLE OF BEHAVIORAL FACTORS 1 (2018), https://www.commonwealthfund.org/sites/default/files/2018-07/Eibner_individual_mandate_repeal.pdf. In 2017 Congress repealed the penalty for noncompliance with the mandate. *Id.*

law (such as the duty of good faith and fair dealing) can influence how the ransom negotiations play out. Part IV elaborates on the argument that ransomware insurance for ransom payments, on balance, is harmful to society. It also complicates the picture by explaining the substantial costs of instituting a comprehensive ban on all ransomware insurance and ransomware payouts, but emphasizes some of the benefits of ransomware insurance, including the risk-spreading and regulatory benefits of such coverage. Part V develops the idea of a limited ban on insurance for ransomware payments, with exceptions (perhaps granted selectively and discreetly by a regulatory body such as the OFAC) for cases involving threats to life and limb, coupled with federally subsidized and mandated coverage for the other costs of ransomware attacks. Part VI briefly concludes.

I. A BRIEF RANSOMWARE OVERVIEW

In 1989 the first ransomware attack locked computers at the World Health Organization's International AIDS Conference.[42] Employing stone-age level sophistication by present standards, the hacker attended the conference and handed out floppy disks to attendees.[43] He told the conference attendees the disks contained a program to predict the risk of contracting AIDS.[44] Once installed, the program had a very simple trigger: after ninety on-off boot-cycles, the ransomware would lock the user's computer and tell the user to send $189 to a post office box in Panama to get the key.[45] The hacker was quickly tracked down and arrested for his crimes, though he was ultimately declared mentally unfit for trial.[46]

The ransomware landscape has changed significantly in the last thirty years as they have become more common and more sophisticated. They have adopted stealthier techniques including threatening to publish sensitive data and using the potential for government fines from disclosure

---

[42] Samantha Murphy Kelly, *The Bizarre Story of the Inventor of Ransomware*, CNN: BUS., https://www.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html (May 16, 2021, 12:46 PM).

[43] *Id.*

[44] Juliana De Groot, *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*, DIGIT. GUARDIAN (Apr. 4, 2022), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

[45] Kelly, *supra* note 42.

[46] *Id.*

of such data to extort payments.[47] Ransomware attacks have also become more expensive. According to estimates, in 2019 ransom demands reached $6.3 billion[48] and the total cost of ransom payments and downtime reached at least $42 billion.[49]

In 2017, ransomware began to make headlines. The WannaCry and NotPetya attacks disabled computers around the globe.[50] WannaCry infected 300,000 computers in 150 countries on six continents.[51] NotPetya has been called "the most devastating cyberattack in history."[52] It froze systems worldwide, including computers at shipping-titan Maersk, pharmaceutical-behemoth Merck, and snack-food giant Mondelez.[53]

---

[47] Lucian Constantin, *More Targeted, Sophisticated and Costly: Why Ransomware Might be Your Biggest Threat*, CSO: ONLINE (Feb. 10, 2020, 3:00 AM), https://www.csoonline.com/article/3518864/more-targeted-sophisticated-and-costly-why-ransomware-might-be-your-biggest-threat.html; Catherine Stupp, *Hackers Get More Sophisticated with Ransomware Attacks*, WALL ST. J. (Dec. 18, 2019, 5:30 AM), https://www.wsj.com/articles/hackers-get-more-sophisticated-with-ransomware-attacks-11576665001.

[48] *Business Interruption Drives 60% of Cyber Losses: Allianz*, BUS. INS. (Nov. 19, 2020, 10:21 AM), https://www.businessinsurance.com/article/20201119/NEWS06/912337901?template=printart.

[49] Jack M. Germain, *New Report Profiles Ransomware Cybergangs*, TECHNEWSWORLD (May 21, 2021, 4:00 AM), https://www.technewsworld.com/story/new-report-profiles-ransomware-cybergangs-87139.html; *Report: The Cost of Ransomware in 2020. A Country-By-Country Analysis*, EMSISOFT: BLOG (Feb. 11, 2020), https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/.

[50] Alex Hern, *WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017*, GUARDIAN (Dec. 30, 2017, 3:00 AM), https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

[51] Selena Larson, *Why WannaCry Ransomware Took Down So Many Businesses*, CNN: BUS. (May 17, 2017, 1:54 PM), https://money.cnn.com/2017/05/17/technology/wannacry-ransomware-business-security/index.html.

[52] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. This particular attack appears to have been coordinated by the Russian government as part of a hybrid warfare campaign initially against Ukraine. Ellen Nakashima, *Russian Military Was Behind "NotPetya" Cyberattack in Ukraine, CIA Concludes,* WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[53] Greenberg, *supra* note 52.

Just as spectacularly as ransomware entered the public consciousness with these two attacks, it fell out of favor with criminals for a period in 2018.[54] Hackers had moved on to other modes of attacks. For example, cryptojacking—the theft of computer resources to mine cryptocurrencies like Bitcoin—increased during this period by 450%.[55] Then, in 2019, ransomware attacks returned with a vengeance.[56]

The lack of mandatory reporting and a centralized information repository makes the scope of the problem difficult to determine.[57] But reports suggest the number of attacks increased in 2019. McAfee Labs reported a 118% increase in ransomware attacks in the first quarter.[58] Criminals captured the public's attention with attacks on major cities, including Atlanta, New Orleans, and Baltimore.[59] Their targets included hospitals in the U.S. and abroad, forcing them to turn away all but the most

---

[54] Danny Palmer, *Cybercrime: Ransomware Attacks Have More Than Doubled This Year*, ZDNET (Aug. 28, 2019), https://www.zdnet.com/article/cyber-crime-ransomware-attacks-have-more-than-doubled-this-year/.

[55] Josh Fruhlinger, *Recent Ransomware Attacks Define the Malware's New Age*, CSO (Feb. 20, 2020, 3:00 AM), https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html.

[56] *See* Barlyn, *supra* note 3 (suggesting spike in 2019); Nathaniel Popper, *Ransomware Attacks Grow, Crippling Cities and Businesses*, N.Y. TIMES (Feb. 9, 2020), https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html ("In 2019, 205,280 organizations submitted files that had been hacked in a ransomware attack — a 41 percent increase from the year before . . . .").

[57] In contrast to the numbers reported in a prior paragraph, an FBI report claimed that losses totaled just over $8.9 million in 2019. FED. BUREAU OF INVESTIGATIONS INTERNET CRIME COMPLIANCE CTR., 2019 INTERNET CRIME REPORT 14 (2019), https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf. The stark difference stems from just 2,047 being reported to the bureau in 2019. *Id.* The number also does not include "lost business, time, wages, files, or equipment, or any third party remediation services acquired by a victim." *Id.* at 20.

[58] CHRISTIAAN BEEK ET AL., MCAFEE LAB THREATS REPORT 1 (Aug. 2019 ed. 2019), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

[59] *See* Popper, *supra* note 56; Manny Fernandez, David E. Sanger & Marina Trahan Martinez, *Ransomware Attacks Are Testing Resolve of Cities Across America*, N.Y. TIMES (Apr. 27, 2021), https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html.

critical patients.[60] In total, "113 state and municipal governments and agencies, 764 healthcare providers, and 89 universities, colleges, and school districts" fell victim to ransomware attacks.[61] Despite the increase, criminals are employing an evolving strategy. Security experts indicate that the number of ransomware detections in businesses rose 365% between the second quarter of 2018 and second quarter of 2019, though consumer detections declined.[62] There is also some evidence the attacks continued to rise during 2020, notwithstanding, or perhaps due to, the Covid-19 pandemic.[63]

Historically, hackers adopted a "spray and pray" opportunistic approach.[64] Criminals used automated systems to send numerous spam emails and fake advertisements hoping to infiltrate users' systems.[65] Once the recipient clicked on the link within these emails and advertisements, the malware downloaded and the user's files were encrypted.[66] The attacks typically were successful in infiltrating individuals' and small businesses' computers—entities with fewer resources to defend their systems.[67] Small ransom demands meant criminals' efforts were only financially worthwhile if a significant number of computers were successfully infected.[68] But

---

[60] *See The State of Ransomware in the US: Report and Statistics 2019*, EMSISOFT: BLOG (Dec. 31, 2019), https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

[61] *Id.*

[62] Alicia DeNisco Rayome, *Ransomware Attacks on Businesses Up 365% This Year*, TECHREPUBLIC (Aug. 8, 2019, 7:00 AM), https://www.techrepublic.com/article/ransomware-attacks-on-businesses-up-365-this-year/.

[63] *See* Brenda R. Sharton, *Ransomware Attacks Are Spiking. Is your Company Prepared?*, HARV. BUS. REV. (May 20, 2021), https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared (citing studies showing that ransomware attacks in 2020 "were up 150% over the previous year" and that the "amount[s] paid by victims of these attacks increased more than 300% in 2020.").

[64] *See* Vadim Sedletsky, *Opportunistic vs. Targeted Ransomware Attacks*, CYBERARK: BLOG (May 12, 2021), https://www.cyberark.com/resources/blog/opportunistic-vs-targeted-ransomware-attacks.

[65] *See id.*

[66] *See id.*

[67] *See id.* (attributing ransomware success rate to lack of proper security hygiene for backups and recovery as well as, companies relying too heavily on traditional anti-virus solutions that is not effective in blocking ransomware).

[68] *See* Lena Yuryna Connolly, David S. Wall, Michael Lang & Bruce Oddson, *An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability*, J. CYBERSECURITY 1, 4 (2020)

criminals are now taking a more targeted approach, focusing on particular business sectors and entities.[69] They are even attacking industrial control systems—the systems responsible for running power grids, manufacturing plants, oil refineries, and sewage treatment plants.[70] They are gaining access to their targets' systems long before releasing the malware.[71] And they are conducting significant reconnaissance to better understand their target.[72] This change in tactic has led to greater success in taking users' files hostage.[73] However, phishing attacks are still widely used.[74] Indeed, several cities that were successfully held for ransom were infiltrated via phishing emails.[75] Ultimately, successful attacks increased by forty-one percent in 2019 from the prior year.[76] Changing tactics have also raised the stakes for entities that are breached, particularly those unwilling to pay ransoms.

In late 2019, reports came out that criminals were no longer just encrypting users' files and demanding a ransom payment; they were now

---

(noting victims are typically asked to pay "an amount that many organizations or individuals can afford to pay, given that the loss of the data is unbearable for the victim.").

[69] *See* Sedletsky, *supra* note 64.

[70] Andy Greenberg, *Mysterious New Ransomware Targets Industrial Control Systems*, WIRED (Feb. 3, 2020, 4:56 PM), https://www.wired.com/story/ekans-ransomware-industrial-control-systems/.

[71] Sedletsky, *supra* note 64.

[72] *Id.*

[73] *See Best Defense Against Spear Phishing Attacks: The Real Dangers of Spear-Phishing Attacks*, FIREEYE, https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html (last visited Apr. 27, 2022) ("People open 3% of their spam and 70% of spear-phishing attempts. And 50% of those who open the spear-phishing emails click on the links within the email—compared to 5% for mass mailings—and they click on those links within an hour of receipt. A campaign of 10 emails has a 90% chance of snaring its target.").

[74] *See* FED. BUREAU OF INVESTIGATIONS INTERNET CRIME COMPLIANCE CTR., 2020 INTERNET CRIME REPORT 3 (2020), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[75] *See, e.g.*, Fernandez, Sanger & Martinez, *supra* note 59 (discussing the Allentown hack via a phishing email); Rachael Thomas, *7 Florida Municipalities Have Fallen Prey to Cyber Attacks Since Last Year*, NAPLES DAILY NEWS (Aug. 20, 2019, 5:14 PM), https://www.naplesnews.com/story/news/crime/2019/08/20/7-florida-municipalities-have-fallen-prey-cyber-attacks-ryuk-ransomware-phishing/2065063001/.

[76] Popper, *supra* note 56.

also downloading and threatening to release sensitive data from the target's system if the victim did not pay the ransom.[77] These threats may significantly alter the calculus to determine whether to pay the ransom. No longer is the high cost of restoring systems the only consequence of not paying the ransom, particularly as criminals make good on their threats. For example, in February 2020, hackers released a trove of confidential data from a personal injury law firm in Texas.[78] The data included, "pain diaries from personal injury cases, fee agreements, HIPPA consent forms, and more."[79] This was not the first time this criminal organization had released data from a victim who refused to pay the ransom. In late 2019, the group released data from Southwire, a cable and wire manufacturer in Georgia, after it refused to pay a $6 million ransom.[80] Despite the company's best efforts, and court orders to stop releasing the information and take down the website, the group continued to publish the data online.[81]

The changing nature of the attacks is also driving up the costs of ransomware. Ransom demands and payments have increased.[82] Other costs

---

[77] *See, e.g.*, Jenni Bergal, *Hackers Threaten to Release Police Records, Knock 911 Offline*, PEW CHARITABLE TRUSTS: STATELINE (May 14, 2021), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/05/14/hackers-threaten-to-release-police-records-knock-911-offline.

[78] Patrick Smith, *Maze Hackers Publish Texas Law Firm's Confidential Data*, LAW.COM (Feb. 11, 2020, 9:44 AM), https://www.law.com/2020/02/11/maze-hackers-delist-texas-law-firm-as-ransom-pressures-mount/.

[79] *Id.*

[80] Jessica Saunders, *Reports: Southwire Incident Was Ransomware Attack Seeking Bitcoin Worth $6M*, BUS. J.: ATLANTA BUS. CHRON. (Dec. 17, 2019, 6:27 AM), https://www.bizjournals.com/atlanta/news/2019/12/17/reports-southwire-incident-was-ransomware-attack.html.

[81] Lawrence Abrams, *Maze Ransomware Publishes 14GB of Stolen Southwire Files*, BLEEPING COMPUT. (Jan. 10, 2020, 5:13 PM), https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/. The group ultimately ceased operations in 2020. Maria Henriquez, *Maze Ransomware Gang Retires*, SEC. MAG. (Nov. 3, 2020), https://www.securitymagazine.com/articles/93819-maze-ransomware-gang-retires.

[82] Indeed, the demands and payments have both reached eight figures. Criminals demanded $70 million to unlock computers affected by REvil group's ransomware attack on Kaseya VSA, a software used by large companies and technology-service providers to manage and distribute updates. Rachel Lerman & Gerrit De Vynck, *Hackers Demand $70 Million to Unlock Businesses Hit by Sprawling Ransomware Attack*, WASH. POST (July 5, 2021, 4:39 PM), https://www.washingtonpost.com/technology/2021/07/05/kayesa-ransomware-70-million-fbi/. The attack affected

are also going up. As these attacks become more sophisticated, costs associated with recovery increase, as does lost revenue and reputational harm. The average length of downtime has increased, reaching as high as sixteen days in the fourth quarter of 2019.[83] Sources attribute this increased downtime to the successful attacks against larger enterprises.[84] As a result, the average cost of downtime in 2020 reached $283,000—an increase of almost 100% from the prior year.[85]

The situation grew worse in 2020. The DOJ declared 2020 the "worst year ever" for extortion-related cybercrimes.[86] According to antivirus firm Emsisoft, the average ransom request reached $200,000 in 2020.[87] Despite the global pandemic that began early in 2020, ransomware attacks focused on hospitals.[88] Attacks were more profitable for ransomware gangs

---

thousands of victims in at least seventeen countries who rely on Kaseya's software. *Id.* And in June 2021, JB USA Holdings Inc., the world's largest meat supplier, actually paid an $11 million dollar ransom demand after cybercriminals took out its processing plants. Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, WALL ST. J. (June 9, 2021, 8:27 PM), https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

[83] *Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate*, COVEWARE (Jan. 23, 2020), https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate.

[84] *Id.*

[85] Aleksandar Kochovski, *Ransomware Statistics, Trends and Facts for 2022 and Beyond*, CLOUDWARDS (Mar. 22, 2022), https://www.cloudwards.net/ransomware-statistics/.

[86] Dustin Volz, *Ransomware Targeted by New Justice Department Task Force*, WALL ST. J. (Apr. 21, 2021, 10:09 AM), https://www.wsj.com/articles/ransomware-targeted-by-new-justice-department-task-force-11619014158?page=1.

[87] *Ransomware Demands Continue to Rise as Data Exfiltration Becomes Common, and Maze Subdues*, COVEWARE (Nov. 4, 2020), https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

[88] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, FED. BUREAU OF INVESTIGATION & DEP'T OF HEALTH & HUM. SERVS., AA20-302A, RANSOMWARE ACTIVITY TARGETING THE HEALTHCARE AND PUBLIC HEALTH SECTOR (2020), https://www.cisa.gov/uscert/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.

too. They made at least $350 million—a 311% increase over 2019.[89] Once again, the criminals laundered their cryptocurrency payments through Bitcoin mixing services.[90] But research suggests that the bulk of that money travels through just a few exchange portals, potentially giving law enforcement an opportunity to disrupt the cash flow of ransomware gangs.[91]

It is difficult to determine how many attacks occur each year, and it is similarly difficult to say for certain what percentage of victims pay the ransom. But a recent survey of businesses found that twenty percent of ransomware victims paid the ransom in 2020—up from only fifteen percent in 2019 and four percent in 2018.[92] Among these, several local governments opted to pay the demand rather than attempt to restore the systems themselves. The city of Riviera Beach, Florida paid the largest of these ransoms—sixty-five bitcoins worth approximately $600,000.[93] Similarly, Lake City, Florida paid forty-two bitcoins worth nearly $500,000 to unlock its systems.[94] Other local governments, however, have not. The city of New

---

[89] KIM GRAUER & HENRY UPDEGRAVE, THE 2021 CRYPTO CRIME REPORT 6 (2021), https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.

[90] *Id.* at 4, 9.

[91] *Id.* at 9, 18.

[92] THREAT POST 2021: THE EVOLUTION OF RANSOMWARE 17 (2021), https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf ("A full 80 percent said they didn't pay the ransom."); DARK READING, HOW DATA BREACHES AFFECT THE ENTERPRISE 12 (2019), https://dsimg.ubm-us.net/envelope/412603/623683/F_1210_P1_13040_DR19_Report_Strategic_Security_2_Data_Breaches.pdf (noting 15 percent paid the demanded ransom in 2019 compared to four percent in 2018).

[93] Benjamin Freed, *Florida City Pays Hackers $600,000 After Ransomware Attack*, STATESCOOP (June 20, 2019), https://statescoop.com/florida-city-pays-hackers-600000-after-ransomware-attack/. The city's insurer negotiated with the hackers and ultimately paid the ransom, leaving the city responsible for only its $25,000 deductible. D. Howard Kass, *Riviera Beach, Florida Ransomware Attack: City Pays $600,000*, MSSP ALERT (June 20, 2019), https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/riviera-beach-florida-malware-attack/.

[94] Catalin Cimpanu, *Second Florida City Pays Giant Ransom to Ransomwarre Gang in a Week*, ZDNET (June 26, 2019), https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/. The city was responsible for its $10,000 deductible. Ian Duncan, *As Florida Cities Use Insurance to Pay $1 Million in Ransoms to Hackers, Baltimore and Maryland Weigh Getting*

Bedford, Massachusetts, for example, chose to restore its systems from backups after hackers demanded more than $5 million in ransom and rejected a counteroffer of $400,000.[95] In addition to the changing size of ransom demands, the form of ransom payment has come a long way since victims were asked to mail a check to a post-office box in 1989.[96] Criminals typically demand payment be made in cryptocurrency—frequently in bitcoin.[97] Indeed, ninety-nine percent of ransoms paid in cryptocurrency in 2019 were delivered using bitcoin.[98]

Introduced in 2008, Bitcoin is a peer-to-peer cryptocurrency that allows rapid, reliable, and *pseudo*-anonymous payments.[99] Cryptocurrency, unlike a traditional bank wire or check-deposit, can be difficult to trace.[100] Indeed, in its early days, Bitcoin was thought to be completely anonymous and untraceable by law enforcement.[101] That myth has slowly unraveled but uncovering the identity of a Bitcoin user remains a difficult task.[102] In fact, some law enforcement officials rely on a criminal's mistakes to track them. In 2013, the FBI was able to identify Ross Ulbricht, the individual behind Silk Road—the dark web's one-stop-shop for illicit goods and services—because he was careless.[103] Ulbricht used a pseudonym for Bitcoin

---

Covered, BALT. SUN (July 5, 2019, 5:00 AM), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-cyber-insurance-20190703-story.html.

[95] Lindsey O'Donnell, *$5.3M Ransomware Demand: Massachusetts City Says No Thanks*, THREATPOST (Sept. 5, 2019, 11:14 AM), https://threatpost.com/ransomware-demand-massachusetts-city-no-thanks/148034/.

[96] *See supra* text accompanying notes 42–46.

[97] *See* MacKenzie Sigalos, *When Ransomware Strikes, This Company Helps Victims Make Bitcoin Payments*, CNBC (June 10, 2021, 3:51 PM), https://www.cnbc.com/2021/06/10/digitalmint-helps-ransomware-victims-make-bitcoin-payments.html.

[98] *Ransomware Payments Up 33% as Maze and Sodinokibi Proliferate in Q1 2020*, COVEWARE (Apr. 29, 2020), https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[99] John Bohannon, *Why Criminals Can't Hide Behind Bitcoin*, SCI. (Mar. 9, 2016), https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin-rev2.

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

transactions that he had adopted years earlier on an internet forum.[104] The FBI was able to use this clue to determine his identity.[105]

Many criminals take extra precautions to make cryptocurrency transactions more difficult to trace, including using "mixing services."[106] These services mix multiple individuals' Bitcoin transactions, functionally laundering the money in an effort to end the trail.[107] "The forensic trail shows the money going in but then goes cold because it is impossible to know which Bitcoins belong to whom on the other end."[108] But even mixing services have exploitable weaknesses when dealing with large sums of money.[109] Despite these issues, transacting in Bitcoin remains a reasonably effective method of masking criminals' identity. New cryptocurrencies hope to address the vulnerabilities in Bitcoin.[110]

In sum, ransomware has become both an enormous source of profit for criminals and an enormous cost for target organizations. It is unsurprising, then, that those organizations would seek to use insurance as a way of helping them manage the risk of ransomware attacks.

II. THE CYBER INSURANCE MARKET

A. THE DEVELOPMENT OF CYBER INSURANCE

It should be no surprise, then, that the significant increase in cyber threats, including the increased threat of ransomware attacks, has fueled a growing market for insurance against cyber-related losses.[111] In the early

---

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.* (discussing Shadow, a new anonymous online market which uses its own cryptocurrency called ShadowCash).

[111] *See* 4 BERT WELLS, RUKESH KORDE & TERESA LEWI, NEW APPLEMAN ON INSURANCE LAW § 29.01(1) (Jeffrey E. Thomas & Aviva Abramovsky eds., Library ed. 2020); Kim Lindros & Ed Tittel, *What is Cyber Insurance and Why You Need It*, CIO (May 4, 2016, 4:43 AM), http://web.archive.org/web/20160505221841/https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html; Adam Janofsky, *Why Companies Should Prepare for More Data Breach Lawsuits*, WALL ST. J. (Dec. 11, 2017, 5:12 PM), https://www.wsj.com/articles/why-companies-should-prepare-for-more-data-

years of cyber-attacks, victims sought coverage for the fall out from cyber-attacks from their commercial property or general liability insurance policies, since those policies (at least the older ones) did not have clear cyber-risk exclusions.[112] Indeed, that is still true for some property and liability policies.[113] Insurers, however, have resisted the effort to find coverage for cyber-related claims under those types of policies, and the results in the courts are mixed. For example, in *America Online, Inc. v. St. Paul Mercury Insurance Co.*, the Fourth Circuit held that computer data, software, and systems were not tangible property under commercial general liability ("CGL") provisions providing property damage coverage.[114] By contrast, in *Computer Corner, Inc. v. Fireman's Fund Insurance Co.*, a New Mexico district court held that data stored on a hard drive did constitute covered tangible property.[115] In 2001, the Insurance Services Office ("ISO")

---

breach-lawsuits-1512563334. There is some evidence, however, that the demand for cyber insurance has levelled off as premiums have risen and budgets have become tighter due to COVID-19. Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem#. Despite a spate of attacks, companies are viewing cyber insurance as a luxury. *Id.* Insurers and reinsurers are also becoming warier about taking on cyber risks—the lack of data and the increasing number and cost of attacks has made the insurance an unattractive proposition. *Id.*

[112] *See* Robert H. Jerry, II & Michele L. Mekel, *Cybercoverage for Cyber-Risks: An Overview of Insurer's Responses to the Perils of E-Commerce*, 8 CONN. INS. L.J. 7, 15–23 (2001) (discussing the evolution of commercial general liability policies through 2001); Anthony R. Zelle & Suzanne M. Whitehead, *Cyber Liability: It's Just a Click Away*, 33 J. INS. REG. 145, 151–52 (2014) (discussing the litigation under pre-2001 commercial general liability policies); 4 WELLS, KORDE & LEWI, *supra* note 111.

[113] *See, e.g.*, Complaint & Demand for Jury Trial, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008 (Ill. Cir. Ct. Oct. 10, 2018); Complaint & Demand for Jury Trial, Merck & Co. v. ACE Am. Ins. Co., No. UNN-L-002682-18 (N.J. Super. Ct. Law Div. Aug. 2, 2018).

[114] Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 96 (4th Cir. 2003). *See also* State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113 (W.D. Okla. 2001) (finding no coverage); Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 115 A.3d 458 (Conn. 2015) (finding no coverage); Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. Lexis 5141 (N.Y. Sup. Ct. Feb. 21, 2014) (finding no coverage).

[115] Comput. Corner, Inc. v. Fireman's Fund Ins. Co., No. CV 97-10380, 2000 WL 35456791 (D.N.M. 2000).

approved a change to the CGL coverage form designed apparently to make it more explicit that cyber risks are excluded.[116]

In the ensuing coverage battles, courts have found no coverage for cyber losses under the post-2001 CGL coverage form. In *Innovak International, Inc. v. Hanover Insurance*, for example, a Florida district court held that a CGL policy provided no coverage when the publication of confidential data was the result of a third-party hacker, rather than the insured.[117] Similarly, in *St. Paul Fire & Marine Insurance v. Rosen*, a federal district judge ruled the insurer did not have a duty to defend under a CGL policy where a data breach was perpetrated by a third party.[118] As a result of similar decisions and the increase in cyber-attacks, the market for standalone cyber risk insurance policies has taken off.[119]

Unlike many insurance policies, which use standardized language, the language within cyber policies often varies between insurance companies and policies.[120] Still, cyber policies do tend to have some characteristics in common. For starters, they all generally provide a variety of first and third-party coverages.[121] Third-party coverage provides insurance for legal liabilities, such as "claims arising out of, or alleging financial loss as a result of a failure of the insured's network security or a failure to protect confidential information."[122] Such insurance fills the coverage gaps left by the post-2001 CGL coverage form, but the frequency or magnitude of such

---

[116] *See, e.g.*, Jeff Woodward, *The 2001 ISO GGL Revision*, INT'L RISK MGMT. INST., INC. (Jan. 2002), https://www.irmi.com/articles/expert-commentary/the-2001-iso-cgl-revision.

[117] Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340, 1349 (M.D. Fla. 2017).

[118] St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., 337 F. Supp. 3d 1176, 1184–86 (M.D. Fla. 2018).

[119] *See* ANDREW GRANATO & ANDY POLACEK, FED. RSRV. BANK OF CHI., CHI. FED LETTER NO. 426, THE GROWTH AND CHALLENGES OF CYBER INSURANCE (2019), https://www.chicagofed.org/publications/chicago-fed-letter/2019/426.

[120] *Id.* at 1.

[121] Shauhin A. Talesh, *Insurance Companies as Corporate Regulators: The Good, the Bad, and the Ugly*, 66 DEPAUL L. REV. 463, 475 (2017) (describing the basics components of a typical cyber insurance policy). First-party coverage pays for an insured's own expenses, including costs related to investigating, reporting, and correcting technological vulnerabilities. GRANATO & POLACEK, *supra* note 119, at 2. Third-party coverage provides protection against legal claims brought by individuals who might be harmed by the attack and who seek to hold the insured-target responsible. *Id.* at 1.

[122] AIG CYBER COVER GUIDE, *supra* note 13.

lawsuits is unclear. First-party cyber coverage can cover a broad range of expenses. For example, cyber policies may provide coverage for the costs of "notifications, public relations, and other services to assist in managing and mitigating a cyber incident,"[123] conducting a forensic investigation to determine the cause of the event, restoring electronic data from backups, business interruption,[124] and ransom payments.[125] At least one insurer provides "towers of coverage"[126]—dividing costs into multiple categories to ensure one kind of expense does not erode coverage for other kinds of expenses.

B. RANSOMWARE INSURANCE[127]

Turning from cyber risk generally to ransomware risk, most modern cyber insurance policies provide some sort of coverage for ransomware attacks. Some companies provide ransomware coverage in their standard cyber insurance policy. For example, AIG offers cyber extortion insurance as part of its *CyberEdge* insurance policy, which provides coverage for a wide variety of cyber risks.[128] That policy defines loss with respect to ransomware attacks to include "monies paid by an Insured with the Insurer's prior written consent to terminate or end a Security Threat or Privacy Threat that would otherwise result in harm to an insured."[129] Other insurers offer cyber extortion endorsements to their general cyber insurance, kidnap-and-ransom, or other insurance policies. Markel, a Virginia-based specialty and small business insurance company, even offers such an endorsement to their

---

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] *Understanding the Coverage*, BEAZLEY, https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response/understanding_the_coverage.html (last visited Apr. 8, 2022).

[127] In Sections B and C, we rely in part on confidential telephone interviews with several attorneys who work as or directly with cyber "breach coaches" in response to ransomware attacks [hereinafter Confidential Interviews with Attorneys].

[128] AIG CYBER COVER GUIDE, *supra* note 13.

[129] AM. INT'L GRP., INC., *CyberEdge Cyber Extortion Insurance*, *in* PORTFOLIO SELECT FOR NON-PROFIT COMPANIES 111, 115 (2013), https://www.aig.com/content/dam/aig/america-canada/us/documents/business/management-liability/portfolioselect-for-public-companies-specimen-policy-brochure.pdf.

"lawyers professional liability insurance policy."[130] That endorsement provides that "[t]he Company shall reimburse the Named Insured up to the amount stated in the Breach Mitigation Expense, Ransomware Attack and Wire Fraud Limits of Liability Schedule as applicable to Ransomware Attack for Loss . . . ."[131] The policy defines a "loss" to include "[t]he Named Insured's payment of an extortion demand."[132] Some insurers appear to offer overlapping coverage, providing for extortion payments in their cyber policies and their kidnap and ransom policies.[133] Coverage under all of these policies is predominantly first-party.

As is the case with many types of property and casualty insurance, cyber insurers do more than simply provide indemnity for loss. They also offer significant expertise and assistance to reduce the insured's cyber risks before attacks happen and reduce their cyber losses after an attack. That is, insurers offer services that are supposed to reduce the likelihood of a successful ransomware attack, and they offer services after an attack occurs, designed to minimize the costs of an attack if one occurs.[134] The former are sometimes referred to as "pre-breach services" and the latter as "post-breach services."[135]

Pre-breach services include access to password management software (which makes it easy for employees to generate and deploy strong passwords to fend off brute force attacks), precision geo-blocking or

---

[130] MARKEL INS. CO., BREACH MITIGATION EXPENSE, RANSOMWARE ATTACK AND WIRE FRAUD COVERAGE (2017) (on file with Journal).

[131] *Id.* at 2.

[132] *Id.* at 5.

[133] *See* Suzanne Barlyn & Carolyn Cohn, *Companies Use Kidnap Insurance to Guard Against Ransomware Attacks*, REUTERS (May 19, 2017, 9:54 AM), https://www.reuters.com/article/us-cyber-attack-insurance/companies-use-kidnap-insurance-to-guard-against-ransomware-attacks-idUSKCN18F1LU. *Compare* TRAVELERS INDEM. CO., KIDNAP AND RANSOM COVERAGE 1 (2016), https://www.travelers.com/iw-documents/apps-forms/kidnap-ransom/ker-16001.pdf [hereinafter TRAVELERS KIDNAP AND RANSOM COVERAGE] (providing coverage for kidnap extortion payments), *with* TRAVELERS INDEM. CO., CYBERRISK COVERAGE 4 (2019), https://www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-16001.pdf [hereinafter TRAVELERS CYBERRISK COVERAGE] (providing coverage for reasonable cyber ransom payouts).

[134] Talesh, *supra* note 121, at 479–84.

[135] *See, e.g.*, Shauhin A. Talesh & 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. 967, 1003 (2021).

shunning (which restricts access to internet sites that are deemed dangerous), and online or in-person cyber security training (designed to teach employees the best practices for avoiding malware attacks and providing a function that allows managers to view employees' test results and completion statistics).[136] In theory, such pre-breach services reduce the risk of a cyber-attack by focusing on the employees—who constitute the weakest link in most organizations' cyber security plans.[137] As Shauhin Talesh has observed, pre-breach services can also include comprehensive "cyber health checks," the goal of which is to "give organizations a 360 degree view of their people, processes and technology, so they can reaffirm that reasonable practices are in place, harden their data security, qualify for network liability and privacy insurance, and bolster their defense posture in the event of class action lawsuits."[138]

Post-breach services offered by insurers also provide potential value to insureds by minimizing the extent of the harm. These services are often provided in the form of an "incident response team."[139] These teams consist of groups of individuals who have expertise in a range of relevant subjects and are employed either by the insurer or by a third-party provider who has

---

[136] *See id.* at 1003–04. Version of these services can be found on the websites of most insurers that sell cyber policies. *See, e.g.*, *Loss Mitigation for Cyber Policyholders*, CHUBB: CYBER SERVICES, https://www.chubb.com/us-en/business-insurance/loss-mitigation-for-cyber-policyholders.html (last visited Apr. 8, 2022); *Cyber Loss Control Services*, AM. INT'L GRP., INC., https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-loss-control-services-all.pdf (last visited Apr. 8, 2022); *Risk Management Tools & Resources*, BEAZLEY GRP., https://www.beazley.com/united_kingdom/cyber_and_tech/beazley_breach_response/cyber_services/risk_management_tools_and_resources.html (last visited Apr. 8, 2022).

[137] *See* Frances Dewing, *Employees Are the Weak Link in Your Business: Why Cybersecurity Protection Starts with Them*, FORBES (Apr. 9, 2019, 8:00 AM), https://www.forbes.com/sites/theyec/2019/04/09/employees-are-the-weak-link-in-your-business-why-cybersecurity-protection-starts-with-them/.

[138] Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY 417, 429 (2018) (quoting NETDILIGENCE, CYBER RISK ASSESSMENTS (2015)).

[139] *See id.* at 432–33. *See, e.g.*, CHUBB, CYBER SERVICES FOR INCIDENT RESPONSE 1 (2020), https://www.chubb.com/content/dam/chubb-sites/chubb-com/ca-fr/claims/marketing-materials/documents/pdf/cyber-servbices-for-incident-response.pdf.

a relationship with the insurer—and whom the insured is incentivized to use through reduced premiums.[140] The services provided by the cyber response team can include forensics, crisis management, public relations, information technology expertise, credit monitoring, and a "breach coach" who runs the show.[141] The breach coach is typically an outside lawyer recommended by the insurer who has experience and expertise in handling a range of legal issues that can arise in the context of a data breach (e.g., intellectual property, privacy law, and national security law).[142] As Talesh notes, "[the breach coach] lawyers play a critical role in developing and managing the incident response team that is formed when a data breach occurs."[143]

In the context of ransomware insurance in particular, the cyber insurer and its cyber response team play an especially critical role in managing the post-breach risk. Someone on the side of the target organization must negotiate with the criminal demanding payment, they must decide whether to pay the ransom, and if a ransom is to be paid, precisely how much that should be, in what form, and under what conditions. While insurers generally leave that process to the insured, the breach coach plays an essential role. Breach coaches oversee the overall response, serving as "central coordinators when it comes to ransomware response, coordinating with computer forensic experts who can determine the extent of the attack, companies that can notify customers impacted by a breach, and IT firms that can quickly provide staffing to fix issues."[144] What's more, if the company decides they do want to pay the ransom (or are at least open to that possibility), the breach coach then brings in a separate ransomware expert, one who has considerable experience negotiating with ransomware attackers and verifying that ransom payments will actually result in unlocked and unharmed files.[145] These experts—who also are not employed by the insurer but are part of the insurer's ransomware response team—play a unique and important role in the response. They can help negotiate for a lower ransom, for example, by deploying specialized negotiation

---

[140] Talesh, *supra* note 121, at 481.

[141] *Id.* at 481–84.

[142] *Id.* at 481–82.

[143] *Id.* at 482.

[144] Steven Melendez, *When Hackers Kidnap Their Data, Companies are Increasingly Using 'Breach Coaches' and Negotiators,* FAST CO. (Mar. 31, 2020), https://www.fastcompany.com/90473369/when-ransomware-strikes-companies-are-increasingly-turning-to-breach-coaches.

[145] *Id.*

strategies.[146] They can also use their own databases,[147] built up over the course of many ransomware negotiations, to determine, among other things, whether a ransom demand is reasonable,[148] whether an attacker is reliable (i.e., whether the encryption keys will actually be provided upon payment), and whether they tend to unlock the frozen data with minimal damage to the files.[149] All of this information is useful to an insured who is trying to minimize their overall losses from ransomware attacks.

C. THE ROLE OF CYBER INSURERS IN RANSOMWARE NEGOTIATIONS

According to one source within the industry that we spoke to, while the typical practice is for insurers not to get directly involved in the ransom-negotiation process, some insurers do.[150] This includes acts such as participating in phone calls between breach coach and client.[151] Even in the typical case, however, where the insurer is remaining "hands off," the presence of the insurance company—and its relationship with the insured and the breach coach—will inevitably have some influence on the negotiation process, at least indirectly. First, if an insured agrees to a ransom demand that the insurer deems to be excessive, the insured runs the risk of either having their premiums increased or losing coverage entirely. Second, the breach coach also has an incentive not to alienate the insurer. Note that in the event of a ransomware attack, cyber insurers typically offer their insureds a panel of attorneys (or potential breach coaches) to choose from.[152] Thus, the insurers clearly have a strong financial incentive to include attorneys in their panel of preferred breach coaches who are able to keep the

---

[146] *Id.*

[147] Confidential Interviews with Attorneys, *supra* note 127.

[148] It might seem odd to think of any ransom demand as being reasonable. All such demands, in an important sense, are deeply unreasonable. By reasonable here we mean something quite specific, which we discuss further below. *See infra* note 161 and accompanying text.

[149] Melendez, *supra* note 144.

[150] Confidential Interviews with Attorneys, *supra* note 127.

[151] *Id.*

[152] Talesh, *supra* note 121, at 482. This is not unlike the practice that liability insurers have in the context of providing legal defense counsel to represent their insureds against covered claims.

insured's—and the insurer's—overall costs down, including the costs of ransom payouts as well as the costs of covering the harm associated with failed ransom negotiations. Therefore, while breach coaches (and the other intermediaries they recommend to the insured to help deal with a ransomware attack) formally represent the insured, and only the insured, they have incentives to consider the interests of the insurer.[153]

The potential role of the cyber insurer in ransom negotiations raises an obvious question. Who does the cyber insurance policy, if at all stated, give ultimate control over the ransom-payment decision? The *contractual authority* to make the final decisions varies from policy to policy. Some policies leave the decision to the insured[154]—this is particularly the case where ransomware is covered as a part of a broader kidnap and ransom insurance.[155] Other policies, including those offered by several major cyber insurers, expressly give the authority to the insurer.[156] Specifically, these policies require the insurer's prior written consent for any ransom paid.[157] Some policies provide this consent requirement in the policy's definition of

---

[153] This is similar to the position of lawyers hired by insurers to defend insureds in a tort action. In "single representation" states (e.g., Hawaii) the attorney has a professional obligation only to the insured. *See* Finley v. Home Ins. Co., 975 P.2d 1145, 1152–53 (Haw. 1998); Pine Island Farmers Coop v. Erstad & Riemer, P.A., 649 N.W.2d 444, 451–52 (Minn. 2002) (finding dual representation is only allowed if there is no conflict of interest and that the insured provides an expressed consent after being informed of the risks and advantages of dual representation, and that there is no conflict of interest); State Farm Mut. Auto. Ins. Co. v. Traver, 980 S.W.2d 625, 632–34 (Tex. 1998). In "dual representation" states, retained counsel represents both the interests of the insurer and the insured, owing a duty to both. *See* Nev. Yellow Cab Corp. v. Eighth Jud. Dist. Ct. *ex rel.* Cnty. of Clark, 152 P.3d 737, 741–42 (Nev. 2007).

[154] *See, e.g.*, TRAVELERS KIDNAP AND RANSOM COVERAGE, *supra* note 133, at 10.

[155] *See* Barlyn & Cohn, *supra* note 133 ("American International Group Inc [], Hiscox Ltd [] and the Travelers Companies Inc [] have been receiving ransomware claims from some customers with K&R policies as ransomware attacks become more common, the companies said.").

[156] *See e.g.*, TRAVELERS CYBERRISK COVERAGE, *supra* note 133, at 4.

[157] These policies stand in stark contrast to kidnap and ransom insurance policies, where kidnap and ransom insurance policies give the final say on whether to pay the ransom to the insured organization or family. *See, e.g.*, TRAVELERS KIDNAP AND RANSOM COVERAGE, *supra* note 133, at 10. We later discuss some differences between kidnap and ransom coverage and ransomware coverage that might help to explain this difference. *See infra* Part IV.B.1.

what is a covered "loss." For example, AIG's *CyberEdge Cyber Extortion Insurance* coverage defines a covered loss as "monies paid by an Insured *with the Insurer's prior written consent* to terminate or end a Security Threat or Privacy Threat that would otherwise result in harm to an Insured."[158]

Note also that, while the policy may require the insurer's consent to any ransom payments, the policy can also impose an obligation on the insurer not to withhold consent unreasonably.[159] Moreover, even if there were no language in the policy expressly imposing a duty of reasonableness on the insurer with respect to ransom-payment decisions, a court could well decide that such a duty is implied in the consent provisions of a cyber insurance policy, just as courts imply a duty of good faith into contracts (e.g., with respect to insurers' "duty to settle").[160]

This combination of rights and responsibilities—where the insurer's consent is required but limits are placed on the insurer's discretion to withhold consent—makes sense from the perspective of maximizing the joint welfare of the insured and insurer named in a particular cyber policy. On the one hand, because the insurer is ultimately responsible for the loss payment, and the amount of the loss payment is a function of the ransom negotiations, the insurer reasonably will want some say in the negotiation process. If the insurer had no such say—that is, if the insured had unfettered

---

[158] *See, e.g.*, AM. INT'L GRP., INC., *supra* note 129, at 115 (emphasis added).

[159] Indeed, this is what AXA's *CyberRiskConnect* policy does. X.L. AM., INC., *supra* note 13, at 10 (stating that insurer's consent "not to be unreasonably withheld . . . ."). Note here the use in the policy of the term "unreasonably" with respect to the decision whether to pay a ransom, implying there are reasonable decisions to pay a ransom and unreasonable ones.

[160] This is especially true because of the potential conflict of interest that can be created by giving unfettered power to the insurer to withhold consent to pay a ransom. Some of the costs of a failed ransom negotiation may not be covered by insurance (either because the expenses fall outside the policy limit or are excluded for some reason), the insurer might externalize some of the costs of a failed negotiation strategy—such as taking too hard a line on what they are willing to pay, resulting in a breakdown of negotiations—to the insured. In the standard liability insurance settlement context, this scenario is sometimes characterized as the insurer gambling with the insured's money. To address the problem in that context, the law applies a duty of good faith and fair dealing, which requires insurers to take into account its own interests and the interests of the insured in such negotiations. *See generally* RESTATEMENT OF THE L. OF LIAB. INS. § 24 (AM. L. INST. 2019) (describing the liability insurer's duty to make reasonable settlement decisions).

control over the ransom negotiation with assurance that any ransom payment would be covered—there would be an incentive for the insured to make an *unreasonable ransom decisions* (i.e., to accede to ransom demands that might, from the perspective of minimizing overall payouts to the hacker, be better to reject).[161] This is a form of moral hazard. But there could also be insurer-side moral hazard if the insurer were given unrestricted discretion to veto any ransom demand that is made. In that situation, the insurer would have an incentive to reject some ransom demands that reasonably ought to be accepted—in the sense that accepting the ransom demand would minimize overall losses associated with this ransom attack.[162] This is why the contract imposes a reasonableness limitation on the insurer's ability to withhold consent for ransom payments. It is also why, if the ransom insurance policy contained no reasonableness limitation, the law would almost certainly imply one as part of the insurer's duty of good faith and fair dealing.[163]

---

[161] By "unreasonable ransom decisions" here, we mean decisions that will tend not to maximize the joint well-being of the two parties to the contract. A reasonable ransom decision, in this context, would be one that is made by a rational party who will suffer all of the losses from a particular ransomware attack. The analogy to the duty to settle context should be obvious. *See* RESTATEMENT OF THE L. OF LIAB. INS. §24(2) (AM. L. INST. 2018) ("A reasonable settlement decision is one that would be made by a reasonable insurer that bears the sole financial responsibility for the full amount of the potential judgment."). As we discuss further below, a ransom decision that might be reasonable from the perspective of the insurer and insured in a particular ransomware situation will not necessarily be socially optimal. *See infra* Part IV.B.1.

[162] This could happen if some of the costs of not paying the ransom are not covered under the insurance policy. In that situation, if the insurer vetoes a ransom demand, it could be because they are, in a sense, gambling with the insured's money.

[163] There are numerous examples of the law implying such a covenant. For example, in almost all liability insurance policies, there is language requiring insureds to get the insurer's consent before settling a claim. 3 FRANKLIN D. CORDELL, NEW APPLEMAN ON INSURANCE LAW § 20.04[2][a] (Jeffrey E. Thomas & Francis J. Mootz, III eds., Library Ed., LEXIS, database updated May 2022). Settlement without consent can result in loss of coverage. *Id.* By the same token, *unreasonable* withholding of consent by the insurer is considered a breach of the duty of good faith. *Id.* § 20.04[2][b]. Similarly, with liability insurance policies that include coverage for defense costs, there are typically provisions conditioning coverage on the insured's not incurring any defense costs without the expressed consent (usually the written consent) of the insurer. *Id.* § 20.04[1][a]. Here too, courts have found that an insurer's unreasonable refusal to grant such consent, even

In sum, although some cyber insurance policies give insurers the power to withhold consent to ransom payments, that power is limited both in the contract itself and, presumably, by the duty of good faith and fair dealing.[164] According to one source we spoke with, however, insurers almost never invoke this contractual authority, preferring instead to defer to the preferences of the insured.[165] This is not surprising for several reasons.

First, insurers may be worried about the possibility of a bad faith claim. That is, if a ransom demand were made that an insured wanted the insurer to pay, but the insurer refused or even delayed, the insurer would run the risk of extra-contractual bad faith liability.[166] Second, insurers have a reputational interest in not being viewed as an obstacle to ransom payouts. It is not uncommon for insurers to pay claims that, strictly speaking, they may not be contractually required to pay, precisely because of this reputational concern.[167] There are obviously limits to this concern, as evidenced by the many coverage disputes insurers do in fact litigate.[168] Third, ransomware insurers, to some extent, rely on the prudence of the breach coaches, who both are experienced in these matters and are likely to have a better sense than most insureds of when a hacker is willing to negotiate and when a ransom demand is unreasonably high (as compared to the costs to the insured of saying no and opting to go the restoration route). Breach coaches, because of their expertise, have a fair amount of influence with the insureds and can often steer them away from making ill-considered ransom-related decisions, such as paying a ransom that could have been successfully negotiated down or declining to accept a ransom demand that is the best offer the insured is likely to get, which would be considerably less expensive than having to restore the overall system. Also, as already mentioned, breach coaches may

---

in the absence of contractual language limiting the insurer's discretion, may be considered a breach of the insurer's duty of good faith and fair dealing. *Id.* § 20.04[1][c].

[164] We say "presumably" because there is no court decision, as of now, applying the duty of good faith and fair dealing to this context.

[165] Confidential Interviews with Attorneys, *supra* note 127.

[166] There is an analogy here to the liability insurer's duty to make reasonable settlement decisions on behalf of an insured against whom a tort claim has been brought. *See generally* RESTATEMENT OF THE L. OF LIAB. INS. § 24(1) (AM. L. INST. 2019) (describing the liability insurer's duty to make reasonable settlement decisions).

[167] Confidential Interviews with Attorneys, *supra* note 127.

[168] *Id.*

have a long-term financial relationship with the insurer, which adds extra incentive for them to prevent the insured from making a decision that would increase the insured's overall costs.[169] Finally, one reason insurers seem never to invoke their contractual veto over ransom decisions is that it is often the insureds who are the ones vetoing any ransom payment.[170] Put simply, the victims of these attacks often react with outrage and anger, and these emotions can translate into an unwillingness to "cave" to the hacker's demands, even when it might be rational for them to do so, given the cost of the ransom and relative to the cost of restoring the system.[171]

III. RANSOMWARE INSURANCE AND THE "EXTORTION ECONOMY": COMPLICATING THE PICTURE

The preceding Part explained the history and the structure of ransomware insurance as a social practice. In this Part we start by reviewing what we call the "profitability complaint," which has been lodged against ransomware insurance coverage for ransom payments. Specifically, the complaint comes from the idea that the presence of insurance makes the business of ransomware more profitable for criminals. Next, we explain why, notwithstanding this complaint, there is at least a theoretical argument that the presence of ransomware insurance might be a social good—or, put in economic terms, welfare enhancing. Nevertheless, we conclude this Part with an argument that there are market failures that may be inhibiting the ability of ransomware insurance to enhance social welfare, giving rise to the case for some form of government action.

---

[169] In fact, we have been told that some cyber policies do not contain consent-to-pay-ransom provisions and that, with respect to those policies, insurers depend even more on the breach coach "to do the right thing" (i.e., to pay the ransom only if it is reasonable). *Id.* One lawyer employed at an "off-panel" firm commented that breach counsel takes some risk by doing this—opening themselves to malpractice suit alleging that the coach failed to advise paying a reasonable ransom, advised paying an unreasonable ransom and causing a subsequent loss of coverage. *Id.*

[170] *Id.*

[171] This assessment was confirmed in a confidential interview with one high-ranking official in an organization that was victimized by a ransomware attack. In that case, the insured decided not to pay the ransom, even though the insurer was willing to pay it and even though forcing the insurer to cover the costs of restoring the system resulted in their premiums doubling the next year.

D. THE PROFITABILITY COMPLAINT

The following is the common-sense intuition that underlies much of the critical reporting on ransomware insurance: the availability of insurance for ransom payments increases the profitability of ransomware attacks and therefore the frequency of such attacks and the amount of ransom demand.[172] This view is based on the notion that entities with ransomware insurance have more money available to pay a potential ransom than entities that do not have such insurance (and that are equal in other respects). The more money a potential cyber target has to spend on a ransom payment, the greater their willingness to pay, and thus the more profitable a ransomware attack will be.[173] The more profitable such attacks are, the more likely those attacks become—assuming the attackers are aware of the presence of ransomware coverage.[174] Indeed, there are media reports suggesting a trend in the

---

[172] Dudley, *supra* note 10.

[173] *Id.*

[174] Whether hackers can determine which targets have ransomware coverage remains something of an open question. Organizations are not required to disclose this information to public sources. However, hackers may be able to figure out who has insurance from non-public sources. The most obvious way to do this would be to hack the insurers themselves and get their list of insureds. There is little doubt that hackers are interested in doing just that. *See, e.g.*, Dmitry Smilyanets, *'I Scrounged Through the Trash Heaps… Now I'm a Millionaire:' An Interview With REvil's Unknown*, THE RECORD (Mar. 16, 2021), https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/ (quoting a representative from ransomware gang REvil that they try to "hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves."). And there have already been a number of hacks of large cyber insurers. *See, e.g.*, Brittany Chang, *One of the Biggest US Insurance Companies Reportedly Paid Hackers $40 Million Ransom After a Cyberattack*, BUS. INSIDER (May 22, 2021, 11:47 AM), https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5 (discussing hacking of CNA). At this point, however, it remains unclear whether the recent hacking of insurance companies has resulted in the criminals getting access to the insurers' list of insureds. Alicia Hope, *Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customers*, CPO MAG. (Apr. 5, 2021), https://www.cpomagazine.com/cyber-security/cyber-insurance-firm-suffers-sophisticated-ransomware-cyber-attack-data-obtained-may-help-hackers-better-target-firms-customers/. What's more, even if hackers succeed in getting the list,

direction of ransomware insurers advising their insureds to pay the ransom, as the "least expensive resolution with the lowest amount of business interruption."[175]

On this view, if the government could raise the costs of paying a ransom—for example, by creating a risk of civil and criminal sanctions for either the insurer or the victims, or both—the amount that the criminals can expect to be paid will go down, and the number of overall attacks should, in turn, decrease.[176] This would be consistent with theoretical predictions that have been made with respect to bans on kidnap-and-ransom insurance.[177] On

---

determining whether the policyholders are covered for ransomware attacks would be a daunting task, as the hackers would have to read reams of pages of densely and obscurely worded insurance policy language. As one internet security expert put it:

> [I]t's premature to talk about a major spike in attacks targeting insurance firms with a purpose to steal lists of customers who have cybersecurity insurance . . . .
>
> . . . .
>
> Moreover, cybercriminals will unlikely go through lengthy cyber insurance contracts to ferret out which specific incidents are covered and what are the numerous exclusions.

Id. (quoting Ilia Kolochenko, CEO, Founder, and Chief Architect of ImmuniWeb).

[175] *See, e.g.*, Scott Ikeda, *Ransomware Attacks are Causing Cyber Insurance Rates to Go Through the Roof; Premiums Up as Much as 25 Percent*, CPO MAG. (Feb. 10, 2020), https://www.cpomagazine.com/cyber-security/ransomware-attacks-are-causing-cyber-insurance-rates-to-go-through-the-roof-premiums-up-as-much-as-25-percent/.

[176] This result assumes that the ransomware "market" is characterized by an upward sloping supply curve, so that the higher the expected ransom payment the greater will be the number of ransomware attacks. Although we are aware of no formal models of the ransomware market, this is how kidnap-and-ransom markets generally are modeled. Parchomovsky & Siegelman, *supra* note 27, at 28–31 (summarizing the literature). Several countries have banned ransom payments in response to organized crime, particularly Colombia and Italy. *Id.* at 29–31. These bans, however, have been in place since 1993 and 1991, respectively, in response to kidnappings in these countries. *Id.*

[177] Game theoretic supports for the presence of ransom insurance increases the willingness to pay of the victims' families. Alexander Fink & Mark Pingle, *Kidnap Insurance and Its Impact on Kidnapping Outcomes*, 160 PUB. CHOICE 481, 490 (2014) (finding that "*the existence of a competitive insurance market increases the maximum ransom demand a family is willing to pay.*"). Parchomovsky and Siegelman note that there is evidence consistent with, though not proof of, the view

the basis of such arguments, some critics of ransomware insurance are so convinced of the harmful effects of ransomware insurance that they have proposed banning it for ransom payments.[178] Others have not gone so far as to call for banning such coverage, though the logical conclusion of their arguments would seem to support a ban.[179] We will have more to say below about calls for a comprehensive ban.[180] But first, consider the argument that, notwithstanding the profitability complaint, the presence of ransomware insurance might at least in theory be welfare enhancing.

E. THE POTENTIAL OF RANSOMWARE INSURANCE

There is an argument, which has been largely missed in the discussions of ransomware insurance, that the existence of a thriving market in this type of coverage could actually increase social welfare, even without any government intervention in the form of bans or subsidies or direct regulation other than the sorts of regulation that apply to all forms of insurance. Let's begin with the risk-spreading benefits of ransomware

---

that banning K&R insurance would reduce kidnappings. Parchomovsky & Siegelman, *supra* note 27, at 31. For example, they note that, in the period following Italy's imposition of severe restrictions on ransom payments, there was a substantial drop in kidnappings. *Id.* at 30. They also point out, however, that that drop in kidnappings could have been the result of "a drop in the rate at which kidnaps were reported to the police." *Id.* at 30 n.111. In conclusion, they summarize the evidence with respect to kidnap-and-ransom insurance as follows: "[t]he bottom line is that while it's difficult to prove that kidnap insurance increases kidnappings, the limited available evidence is entirely consistent with that possibility, and some theoretical models predict it." *Id.* at 31.

[178] Perhaps the most well-known example of this involves Ciaran Martin, the former head of the National Cyber Security Centre. *See* Sabbagh, *supra* note 23; Gareth Corfield, *How Do We Stamp Out the Ransomware Business Model? Ban Insurance Payouts for One, Says Ex-GCHQ Director*, REGISTER (Apr. 9, 2021, 10:02 AM), https://www.theregister.com/2021/04/09/ban_cyber_insurance_payouts/; Scroxton, *supra* note 15.

[179] The *ProPublica* story would be an example of this. Dudley, *supra* note 10. A research paper released by the Royal United Services Institute makes much the same argument—that cyber insurance policies are encouraging cybercriminals. JAMIE MACCOLL, JASON R. C. NURSE & JAMES SULLIVAN, CYBER INSURANCE AND THE CYBER SECURITY CHALLENGE 38, (2021), https://static.rusi.org/247-op-cyber-insurance-v2.pdf.

[180] *See infra* Part IV.B.3.

insurance. Even if it is true that the presence of ransomware insurance increases the likelihood of an attack and the amount of the payouts, there are potential welfare gains from taking the risks of cyber-attack experienced by individual organizations and spread those risk over much larger pool of insureds through an insurance contract. What's more, it is at least possible that the gains from risk distribution can more than offset any increase in losses due to moral hazard. This is a standard move in the economic analysis of insurance. Indeed, even the economists who model ransom situations conclude that as a result of the risk-spreading benefits of kidnapping insurance, the efficient outcome would be at least partial coverage despite the possible moral hazard effect.[181]

In addition to the obvious risk-spreading benefits of ransomware insurance, there is also the possibility that the presence of insurance could actually reduce rather than increase the likelihood of an attack or the severity of its consequences.[182] How is this possible? The argument builds on the observation, first, that private insurance companies have a financial incentive to find ways to lower their insureds insured losses. For example, if an insurer can, by encouraging simple risk-reducing behavior on the part of their customers, lower the price they pay for insurance, that insurer can compete those customers away from, or prevent them from being competed away by, other insurers. [183] Also, once an insurer has collected a premium for a given policy period, any changes in behavior on the part of the insured that reduce the insured risk for that period will redound to the financial benefit of the insurer.[184]

---

[181] *See, e.g.*, Fink & Pingle, *supra* note 177, at 498.

[182] Parchomovsky and Siegelman, in their discussion of the third-party moral hazard effects of K&R insurance, discuss the possibility of insurers helping their insureds to reduce their vulnerability to kidnapping. Parchomovsky & Siegelman, *supra* note 27, at 45–49 (discussing loss control and monitoring by insurers).

[183] Ben-Shahar & Logue, *supra* note 37, at 203–05 (discussing insurers' financial incentives to find ways to reduce their insureds risks). Below, however, we discuss how particular market failures may be muting those incentives. *See infra* notes 237–42 and accompanying text.

[184] Ben-Shahar & Logue, *supra* note 37, at 203–05. We are, of course, not saying that insurance companies' interest in maximizing profit is coextensive with society's interest in reducing ransomware attacks. If all insurable risks were somehow miraculously eliminated, society would be better off, but insurers would be out of business. The same sort of point could be about the medical profession (if all diseases were magically eliminated) or law enforcement (if all crime was eliminated). The profit interests of insurers and the interests of society diverge at

In addition to having some incentive to reduce their insured's risks, insurance companies also have tools with which to do so. Some of those "regulatory" tools operate *ex ante*—that is, the insurers take steps before the loss event happens that reduce the probability or magnitude of the loss—and some of the tools operate *ex post*—that is, the insurers take steps after the loss event happens to minimize the size of the loss.[185] As for the *ex ante* tools, recall the earlier discussion of all the pre-breach services the cyber insurers are offering their insureds.[186] To the extent insurers, through premium discounts or otherwise, can incentivize organizations to adopt essential pre-breach cyber security best practices (i.e., investing in state-of-the-art backup systems, endpoint and anti-virus protection, and security awareness training for all employees),[187] they may actually reduce, rather than increase, the overall threat of ransomware attacks.

As for *ex post* tools, recall the earlier discussion of the critical role played by insurers' post-breaching consulting, as they bring in breach coaches, forensic experts, public relations experts, privacy law experts, and ransom negotiators to assist with all aspects of the cyber breach.[188] With

---

some point. Specifically, if the risk of ransomware attack were to get sufficiently low, there is a sense in which it may no longer be in the profit-maximizing interest of the insurance industry to look for ways to reduce the risk further. However, it also seems likely that, for risks that are reasonably large and unlikely to be reduced to anything close to zero any time soon—that is to say, for most of the risks that can profitably be insured by a private insurance company—there is a wide range of overlap between the insurers' interests, the insureds' interest, and society's interests. This certainly seems true for the rapidly growing risk of ransomware attacks.

[185] For a general discussion of how private insurance companies engage in what amounts to *ex ante* and *ex post* regulation that is similar, though not identical government regulation, see *id.* at 205–16. Insurers resist the notion that their efforts at helping insureds engage in risk- or loss-mitigation represents a form of regulation, perhaps because, if they become too involved, they (the insurers) may be held responsible beyond the coverage they have agreed to in their insurance policies. *See* Kyle D. Logue, *Encouraging Insurers to Regulate: The Role (If Any) for Tort Law*, 5 U.C. IRVINE L. REV. 1355, 1357–58 (2015).

[186] *See supra* notes 136–38 and accompanying text.

[187] *Corporate Ransomware Response & Protection Best Practices*, COVEWARE (Dec. 19, 2018), https://www.coveware.com/blog/2018/12/19/definitive-guide-to-corporate-ransomware-response-amp-protection-best-practices. Some experts believe that practicing the backups adds security. Confidential Interviews with Attorneys, *supra* note 127.

[188] *See supra* notes 139–49 and accompanying text.

respect to this type of intervention, Talesh concluded that "[p]erhaps the biggest intervention the insurance field makes is the array of risk management services it offers to shape the way that organizations *respond* in the event of an actual data breach."[189] The active role played by insurers in *ex post* loss mitigation is unsurprising given the economic incentives faced by insurers. An insurer who is contractually obligated to reimburse any ransom payouts, as well as the cost of any failed ransom negotiations (such as the cost of restoring the insured's locked data, as well as the insured's business interruption losses and liability claims) will have a contractual incentive to help their insureds respond in a way that minimizes the insureds' covered costs. Further, the insurer, through the operation of insurance law (specifically, the duty of good faith and fair dealing) as well as competitive insurance markets (and the desire to maintain a good commercial reputation), will have an incentive to manage the ransomware attack in a way that takes account of the insureds' uncovered costs as well.[190] Thus, taking all of these incentives into account, the insurer should be incentivized to pay the ransom—or to encourage the insured to pay the ransom—when that payment will be less than the expected costs to the parties of not paying the ransom. At the same time, the insurer will have an incentive to refuse to give consent to a ransom (where the contract gives the insurer that authority), or an incentive to encourage the insured to refuse to pay the ransom (where the contract gives the insured the final say), when doing so minimizes the parties' overall costs.

Besides these *ex ante* and *ex post* "regulatory" tools that insurers can, and have some incentive, to deploy in order to reduce ransomware risks, there is another way in which the presence of cyber insurance can reduce the likelihood of a ransomware attack. It has to do with the risk-distribution effect of the coverage for the costs of ransomware attacks other than the payment of the ransom itself. To the extent that cyber policies provide first-party and third-party coverage against the business interruption costs of having one's computer system locked for an extended period of time, repairing and restoring that system, and covering liabilities arising out of such costs, the expected cost to an insured organization of a potential ransomware attack is lessened. That is to say, while having coverage for the ransom payment increases the pot of money available to pay the ransom—and at least potentially increase the profitability to criminals of engaging in ransomware attacks—the coverage for the costs of ransomware attacks

---

[189] Talesh, *supra* note 138, at 432.

[190] *See supra* notes 161–63 and accompanying text for previous discussion of the duty to make *reasonable* ransom negotiation decisions.

increases the pot of money for the insured *not* to pay the ransom, producing the opposite effect on the profitability of the criminal enterprise.

In sum, given the risk-spreading and potential risk-reducing benefits associated with the presence of ransomware coverage, one might be tempted to conclude—contrary to the tone of the recent reporting—that the cyber insurance market should be left alone to work its magic. That conclusion should be resisted, however, because of the presence of (at least) two market failures, two externalities to be precise: the single-year-policy externality and the ransom externality.

The vast majority of property and casualty insurance policies, including cyber policies, are written on a one-year basis. As a result, insurers, when pricing the risk for a single year, will have a tendency to undervalue losses that their insureds might incur that are likely to fall outside of that one-year coverage period since the insurer will not be responsible for covering those costs. We say "undervalue" rather than totally ignore because of the probabilistic nature of insured losses. That is, whether a given loss to an insured will occur outside or inside the coverage period will be, to some extent, stochastic; and, to the extent that is the case, the insurer would have some (albeit probabilistically discounted) incentive to take those losses into account. Still, some portion of an insured's future losses will be expected to fall outside of the insured period. And here is the problem with those losses in particular: there may be *ex ante* investments in enhanced safety by the insured that would reduce or eliminate the risk of such losses that the insurer is aware of (because of its relative expertise in such matters compared with some insureds) but that the insurer will not be induced to fully incentivize (through premium discounts, say) because the cost of such risk-reduction investments need to be amortized over several years.

This point can be illustrated with a simple example. Assume that an insured faces a risk of loss that will with certainty (if it happens at all) happen within the period of the single-year-policy issued by the insurer. Assume further (a) that this risk has an *ex ante* expected cost of $100; (b) is fully covered under the policy; but (c) can be eliminated with a pre-loss investment by the insured of $70. The insurer in such a scenario would have an incentive to encourage the insured to make the $70 risk-reducing investment by offering the insured a premium discount of somewhere between $70 and $100. This is because the insurer would get the full $100 expected benefit of the investment. However, here is the problem: if we changed the hypothetical so that the insured faced a risk of loss that still had an expected cost of $100 but that had an equal probability of happening in any year over the next 5 years, the insurer would not have an incentive to

offer the necessary discount. This is because some of the benefit of the insured's investment—and of the insurer's premium discount—would be externalized to future years, when the insurer might not be covering the risk. Indeed, an insurer in this situation, were they to provide a large up-front premium discount to encourage such an investment in long-term enhanced safety, would find themselves at a pricing disadvantage compared with competing insurers in future years, as those firms would not have incurred the cost of providing what amounts to a subsidy to the insured. It is this very possibility—of not being able to recover the cost of investments that produce safety benefits beyond the end of the policy period—that discourages the insurer from offering such premium discounts in the first instance.[191]

The second obstacle to the "leave the ransomware insurance market alone" argument is what Anja Shortland calls the "ransom externality."[192] While the insurer and insured enjoy all or at least most of the benefits of paying the ransom demand—that is, the benefits of receiving the decryption key from the hacker—they bear only the out-of-pocket costs of doing so. That is, they will generally ignore the cost to society of increasing the incentive for future ransomware attacks. In other words, to use Parchomovsky and Siegelman's terminology, they will ignore the third-party moral hazard effect.[193] This externality can affect insurers' and insureds' incentives in a number of ways. Most obviously, at the *ex post* stage, once the attack has occurred and the ransom demand has been received, the insurer and insured may be willing to pay ransom payments that are efficient or

---

[191] A similar externality arises because of the inability of insurers to get intellectual property protection for their investments in risk detection, mitigation, and pricing technologies. *See, e.g.*, Joe Van Acker, *Fed. Circ. Upholds PTAB's Invalidation of Progressive's IP*, LAW360 (Aug. 24, 2015, 3:27 PM), https://www.law360.com/articles/694435/fed-circ-upholds-ptab-s-invalidation-of-progressive-s-ip. This is not a problem that is peculiar to the cyber insurance market. Most forms of property and casualty insurance are sold on an annual basis, which means this externality has the potential to affect insurers' incentives with respect to many different types of risks. Scholars have long observed, for example, that because homeowners' insurance policies are sold on an annual basis, an externality arises. HOWARD C. KUNREUTHER, ERWANN O. MICHEL-KERJAN, NEIL A. DOHERTY, MARTIN F. GRACE, ROBERT W. KLEIN & MARK V. PAULY, AT WAR WITH THE WEATHER: MANAGING LARGE-SCALE RISKS IN A NEW ERA OF CATASTROPHES 361–65 (Carol Heller ed., Wharton Risk Management & Decisions Processes Center ed. 2008).

[192] SHORTLAND, *supra* note 11, at 171.

[193] *See* Parchomovsky & Siegelman, *supra* note 27, at 4.

joint-wealth maximizing from their perspective but are inefficient from the broader societal perspective.

To see this point, consider another fanciful but illustrative example. Imagine that all ransomware attacks were covered fully by insurance, and that all such insurance were provided (and were expected to be provided for the foreseeable future) by a single giant cyber insurance company. In that case whenever there was a ransomware attack, the insurer's incentive on whether to pay the ransom and how much to pay would be roughly coextensive with society's interests. Since the insurer would bear all of the costs and benefits of the decision to pay the ransom or not, the insurer's decisions whether to pay the ransom or not will be closer to the social optimum than would be the case if some of those costs are externalized.[194] Thus, if paying any given ransom increased the expected cost to all possible future victims of ransomware attacks (because of the perceived increase in the profitability of such attacks) by more than the expected cost of refusing to pay the ransom (the cost of rebuilding the insured's network and covering business interruption costs in the meantime), then the insurer would be likely to reject the ransom. If the reverse were true, it would be likely to pay the ransom. But once we take account of the fact that every individual insurer bears only a (presumably) very small fraction of the costs resulting from the increased demand for ransomware attacks produced by their decision to pay a given ransom, they will tend to pay ransoms more often (and to pay larger amounts in ransom) than is socially cost justified.[195] That is the ransom externality at the *ex post* or post-breach stage of the ransomware attack. There can also be effects at the *ex ante* or pre-breach stage. For example, if the insurer and insured know that they can always pay the ransomware hackers' demanded price—while externalizing most of the resulting third-

---

[194] The incentives of insurance companies, of course, will never be coextensive with what maximizes overall social welfare. This can be seen most clearly by recognizing that insurers would be put out of business entirely as underwriters of risk if the risks that they insure were eliminated, even if eliminating such risk would be social welfare maximizing.

[195] This is also sometimes referred to as a problem of "dynamic inconsistency," which means that it might be rationale to make one decision at one point in time (i.e., refuse to pay ransoms generally to discourage ransomware attacks), but then it becomes rational to do the opposite at a different point in time (i.e., once one is the victim of a ransomware attack, it becomes individually though not socially rational to pay the ransom). Parachomovsky & Siegelman, *supra* note 27, at 34.

party moral hazard costs of that decision—their incentive to invest in *ex ante* prevention would also be undermined.

Is there any evidence that the single-year-policy and the ransom externalities are currently causing insurers to underinvest in *ex ante* risk or *ex post* loss reduction efforts? No direct evidence exists of this connection, so far as we are aware. There is, however, recent evidence that insurance companies in the cyber insurance markets are doing less *ex ante* risk regulation than one might have expected. According to a recent empirical study conducted by Shauhin Talesh and Bryan Cunningham, which included interviews of some sixty people in the cyber insurance field, most insurers are reluctant to require their insureds to adopt pre-breach risk-mitigating best practices.[196] They found, for example, that while insurers are generally making use of big data, predictive analytics, and AI to better assess the risks of cyber insureds, most insurers seem to be unwilling to require that their insureds make use of the insurer's pre-breach services in order to get premium discounts or to qualify for coverage at all.[197] Instead, most insurers are merely offering those pre-breach services as options. What's more, Talesh and Cunningham found that the vast majority of insureds are, in fact, declining those services.[198] As a result, they conclude that "cyber insurers

---

[196] Talesh & Cunningham, *supra* note 135, at 1003–04, 1014.

[197] *Id.*

[198] *Id.* at 1015 (finding that "fewer than 10 percent of insureds that purchase cyber insurance actually use the vast array of pre-breach services insurers offer that would potentially reduce the insured's potential risk . . . ."). These findings are somewhat in tension with Talesh's earlier article on the subject, published in 2017, where he concluded:

> These risk prevention tools and security ratings play an important regulatory role over organizations. First, the scans and health checks are sometimes used as a precondition for determining whether a potential company is eligible for cyber insurance. Organizations interested in insurance protection, therefore, are often interested in becoming more cyber secure. Second, the better a company scores on its health check, the greater the likelihood the insurance company will lower its premiums.

Talesh, *supra* note 138, at 429. In his defense, Talesh in that paper acknowledges in a footnote that, because cyber insurance is not yet a mature insurance market, insurers do not have the "refined premium setting standards" that they have for other lines of coverage. *Id.* n.13. But based on his field research at the time, "the more cyber secure organizations are with good preventative tools in place, the more likely

role as quasi-regulators is largely ineffective—so far."[199] They attribute the insurer's reluctance to insist that their insureds engage in cyber security best practices to the "soft market" in property and casualty insurance and the threat that the insured will simply switch to another insurer, as well as to the insurers' insistence on continuing to use some traditional underwriting practices, such as focusing on past behavior and limiting the underwriting (and risk-assessment) process to once a year, neither of which responds to the "constantly evolving" nature of cyber risk.[200]

---

organizations would be issued insurance and receive a favorable pricing arrangement." *Id.*

[199] Talesh & Cunningham, *supra* note 135, at 1015. They also conclude that most cyber insurers, in doing pre-breach risk assessments, although they are relying on big data, predictive analytics, and even AI, are using unreliable databases and, worse, are using those data misleadingly to encourage insureds to purchase higher policy limits rather than to encourage insureds' to engage in risk reduction. *Id.* at 1007–11. These are both potentially serious problems that may warrant regulatory intervention, although, as Talesh and Cunningham point out, the regulators will often find themselves using the same imperfect databases in making their regulatory decisions. *Id.* at 1017–19. Talesh and Cunningham also lament the fact that insurers do not seem to check the veracity of statements being made on insurance applications, tending instead to rely on doing so only for those subset of cases where a claim is filed. *Id.* at 995, 1016–17. Such ex-post underwriting, however, at least in cases involving relatively sophisticated parties, may not be problematic, but could be seen as another form of cost-saving *ex post* regulation. *See* Ben-Shahar & Logue, *supra* note 37, at 215–16.

[200] Talesh & Cunningham, *supra* note 135, at 1015–17. Kenneth Abraham and Daniel Schwarcz consider this issue as well. They suggest that the reluctance of insurers to engage in a greater degree of *ex ante* regulation stems from what they call the "cyber insurance gap," the fact that "cyber insurers typically insist on setting policy limits that are well below policyholders' economic exposures to cyber risk." Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe*, 27 CONN. INS. L.J. 1, 54 (2021). Because of this gap in cyber coverage, they argue:

> It is difficult for cyber insurers to insist on meaningful changes to policyholders' cybersecurity precautions if they are only covering a small percentage of the risks that may flow from a cyberattack to that firm. Relatively low coverage limits also make it harder for cyber insurers to insist that firms collect their own data regarding cyber exposure as part of the underwriting process. Additionally, the relatively small amount of capital that insurers have devoted

Interestingly, Talesh and Cunningham are not overall pessimistic about the role of cyber insurers as *ex ante* risk regulators. Rather, they conclude that insurers may serve a "meaningful" role if they follow these recommendations:

> (1) engage in continuous evaluation and underwriting throughout the life of cyber insurance policies, (2) make insurance premium pricing contingent on reliable evidence of good cybersecurity practices (i.e., reward good behavior with reduced premiums), (3) when necessary, require prospective insureds to make changes to improve their cybersecurity posture as a prerequisite to issuing insurance, and (4) engage in dynamic risk management and loss control throughout the policy period to reduce insureds' risk of loss.[201]

Thus, insurers must not only add real carrots and sticks to their *ex ante* regulation—in the form of substantial premium discounts and compliance mandates, respectively—but also engage in such regulation continuously, making adjustments to their premium-discount offers and risk-reduction mandates as the AI-infused analysis of the constantly changing data, and constantly changing cyber-risk landscape evolve over time. In support of this relatively hopeful assessment, Talesh and Cunningham report that at least some relatively new insurance companies are charting a path very much in line with their recommendations and "with modest success."[202]

> to cyber insurance means that collective insurance industry investment in understanding, protecting against, and informing others about cybersecurity is correspondingly limited.

Id. at 56–57 (footnotes omitted). In other words, until cyber insurers have more skin in the game (i.e., offer higher policy limits), they will lack the incentive to encourage better cyber hygiene on the part of their insureds. Abraham and Schwarcz suggest a number of possible ways in which the cyber insurance gap might be closed, including the introduction of a federal backstop. *Id.* at 57–66. *See infra* Part IV.B.3 for our discussion of a similar federal backstop idea.

[201] Talesh & Cunningham, *supra* note 135, at 1020.

[202] *Id.* at 1020–21. Specifically, they conclude that, if insurers fully embrace the promise of new technology (including big data and AI), they can, in theory, "help increase organizations' cybersecurity and insurer's ability to play a positive regulatory role." *Id.* at 1020. The companies that are cited as exemplars of the newer, more modern, more risk-reducing approach to insuring cyber-related risk are At-Bay

IV. A POSSIBLE WAY FORWARD: OF LIMITED BANS (AND MANDATES)

Let us summarize where we are. Ransomware attacks present an enormous social problem. Some commentators have expressed concern that the existence of insurance for ransomware attacks makes the problem worse by providing a pot of money that makes the ransomware business, from an expected value perspective, more profitable for criminals than it would otherwise be.[203] In response we have made a series of observations. On the one hand, it is at least possible that the presence of insurance produces overall welfare gains, either as a result of risk distribution (through the shifting of the risk of attacks from relatively risk-averse insureds to relatively risk-neutral insurers) and risk minimization (through the provision of expert pre-breach and post-breach cyber services by insurance companies, who have a stake in seeing those risks get reduced). On the other hand, there remain reasons to be worried. The single-year-policy externality and the ransom externality (or third-party moral hazard problem) are serious concerns, and they threaten to undermine insurers' incentives to engage in an efficient level of pre-breach and post-breach risk minimization. Indeed, there is some suggestive, albeit far from conclusive, evidence that these concerns may currently be inhibiting cyber insurers' incentives to regulate risk, as revealed in Talesh and Cunningham's work discussed above.[204]

These observations lead to the next set of questions. First, might there be a private ordering or Coasian solution to these problems—a way in which the market itself could internalize these externalities? Second, if the answer to that question is no, what government regulatory intervention might be worth considering and what the costs and benefits of such government

---

and Coalition, Inc. *Id.* at 1020. As one example of At-Bay's risk-reducing innovations, they constantly monitor their insureds' remote desktop protocol (RDP) ports, which were the source of twenty-five percent of ransomware losses in 2018 and 2019. *Id.* at 1024. If the insured has not closed all of its RDP ports, At-Bay apparently suspends their coverage. *Id.* This sort of continuous monitoring and continuously enforced cyber security protocols represent the *ex ante* regulatory potential of cyber insurers.

[203] *See supra* Part III.A.

[204] *See supra* notes 196–202 and accompanying text.

intervention might be? Although answering those questions fully is beyond the scope of this (or any single) Article, this Part begins that discussion.

A. RESPONDING TO THE SINGLE-YEAR-POLICY EXTERNALITY

A solution to the single-year-policy externality is easy enough to describe: property and casualty insurers just need to start selling multi-year insurance policies, including (for current purposes) cyber policies. The more years that are covered under a given policy, the smaller the potential externality, all else equal.[205] For this to happen organically, without government involvement, we have to imagine a scenario in which it becomes profit-maximizing for property and casualty insurance companies to offer multi-year insurance policies. This is not inconceivable. Scholars have developed plausible models of insurance markets in which both single-year and multi-year policies could emerge.[206] Indeed, some insurers sell multi-year policies for some types of coverage, including management liability, financial institution bond insurance and, in some countries, homeowners insurance.[207] These markets emerge, in part, because of the perceived benefits to policyholders of locking in premiums and avoiding the hassle of going through a policy renewal.[208] To the extent such policies already are in use, they ameliorate the single-year-policy externality.[209]

---

[205] If the increase in number of years of coverage were accompanied by lower policy limits, then the externality would re-emerge in a different form.

[206] *See, e.g.*, Paul R. Kleindorfer, Howard Kunreuther & Chieh Ou-Yang, *Single-Year and Multi-Year Insurance Policies in a Competitive Market*, 45 J. RISK & UNCERTAINTY 51 (2012).

[207] *See, e.g.*, JOE CATALANO, COMMUNITY BANKS: THE RETURN OF THE MULTI-YEAR INSURANCE POLICY 1 (2016), https://www.amwins.com/docs/default-source/insights/client-advisory_community-banks-the-return-of-the-multi-year-policy_7-16.pdf?sfvrsn=1333ec5f_0 (describing re-emergence of multi-year liability policies after market recovery from 2008 financial crisis); Fiona Reddan, *Multi-Year Insurance Deals — Do They Make Sense?*, IRISH TIMES (Aug. 2, 2016, 6:00 PM), https://www.irishtimes.com/business/personal-finance/multi-year-insurance-deals-do-they-make-sense-1.2736307 (describing Irish market for multi-year homeowners policies).

[208] Kleindorfer, Kunreuther & Ou-Yang, *supra* note 206, at 52.

[209] Scholars have long touted the potential benefit of "long-term homeowners' insurance" as a way of forcing insurers to take into account the fluctuating nature of catastrophic losses over time. *See, e.g.*, KUNREUTHER, MICHEL-KERJAN, DOHERTY, GRACE, KLEIN & PAULY, *supra* note 191, at 367–71. Though the idea was not offered

The market for multi-year property and casualty insurance generally, and in the cyber market in particular, however, has not taken off on its own. The vast majority of policies are still sold on a single-year basis.[210] And reasons for that are understandable. First, if a risk being insured is highly volatile from one year to the next (as cyber risk is), making pricing even a single-year-policy difficult, then pricing a multi-year policy for that risk would be even more difficult. As a result, an insurer offering multi-year cyber policies would need to charge a serious mark-up over its single-year premiums to cover this uncertainty; or the insurer would have to maintain a very large capital base to cover any pricing errors; or they would do both.[211] This will generally limit the demand for multi-year contracts, at least in the primary retail insurance market.[212] And the presence of the single-year externality only makes this problem worse. That is, the presence of the externality will push up prices for long-term insurance even more, further depressing demand for such coverage.

What role might government play, then, in encouraging or fostering the purchase of multi-year cyber policies? The federal government could encourage property and casualty insurers to offer cyber coverage for policy periods longer than one year by agreeing to provide federally subsidized reinsurance for such coverage or through other, more direct subsidies. More drastically, insurers could be required to offer such policies as an option, with subsidies designed to make the coverage more affordable. Such proposals come with costs and benefits, of course.[213] One argument against the adoption of a multi-year policy subsidy or mandate is that, in addition to the examples of multi-year policies already in existence (discussed above),

---

to deal with the externality discussed here, but rather to force insurers to take into account the fluctuations in catastrophic losses over time. *Id.*

[210] Kleindorfer, Kunreuther & Ou-Yang, *supra* note 206, at 52.

[211] Trevor Maynard & Nicola Ranger, *What Role for "Long-Term Insurance" in Adaptation? An Analysis of the Prospects for and Pricing of Multi-Year Insurance Contracts*, 37 GENEVA PAPERS 318 (2012).

[212] *Id.* at 332. Reinsurance companies do offer multi-year policies, which may internalize some of the single-year policy externality, insofar as reinsurers provide a sort of coordinating function among primary insurers. *See infra* notes 219–30 and accompanying text for discussion of Lloyd's role in K&R insurance. *See, e.g.*, *Multi-Year Multi-Line Insurance Covers*, SWISS RE: CORP. SOLS., https://corporatesolutions.swissre.com/innovative-risk-solutions/multi-year-multi-line-covers.html (last visited Apr. 10, 2022).

[213] *See infra* IV.B.3 for discussion on such subsidy and mandate ideas.

perhaps the insurance market already provides something similar to multi-year policies on a much broader scale. That is, even without multi-year contracts, the single-year-policy externality is ameliorated insofar as there are costs to switching insurers. This is because when an organization decides to switch property and casualty insurers, the new insurer will require the insured to go through the underwriting process and may presume, in the absence of good evidence to the contrary, that the switch is for adverse selection reasons. This fact can lead to a mutual expectation that insureds will tend to stay with the same insurer over time, at least for a few years, which has some of the same cost-internalizing benefits of a multi-year policy subsidy or mandate.[214] For this reason, enacting some regulatory response to the single-year-policy externality may not strictly be necessary.

B. RESPONDING TO THE RANSOM EXTERNALITY

1. Lessons from Kidnap-and-Ransom Insurance

The ransom externality—which is, of course, the key to the extortion economy argument in favor of a ban—is a separate, and potentially more serious concern that may require a substantial regulatory intervention. What is needed is a way to internalize to cyber insurers and their insureds the cost of the third-party moral hazard effects of their ransom payment decisions.[215] One potential source of cost-internalization, which seems to be working in the K&R insurance market, is coordination within the reinsurance industry.[216] K&R insurance presents a very similar third-party moral hazard problem. Insurance companies provide coverage against the possibility of an individual being kidnapped, and the coverage provides not only money to pay the ransom, but the services of various professionals, including expert advice about how to avoid getting kidnapped as well as the guidance of professional ransom negotiators.[217] If a kidnapping does occur, there is obviously a strong incentive, felt by the insurer as well as the family of the

---

[214] Also, to the extent a multi-year policy mandate would increase costs, perhaps that cost increase could be spread further through the federal cyber insurance backstop that we discuss below. *See infra* 249–54 and accompanying text.

[215] To use Parchomovsky and Siegleman's language. Parchomovsky & Siegelman, *supra* note 27.

[216] *See generally* SHORTLAND, *supra* note 11, at 67–78 (describing the ways in which the reinsurance markets, especially through Lloyd's, provides a form of "private governance" to internalize the ransom externality).

[217] *Id.*

victim, to pay the ransom so as to avoid the death of the victim—a loss that obviously cannot be fully compensated by any form of insurance. At the same time, the direct insurer and the insured will tend to ignore—or externalize—the effect of paying the ransom on future kidnappings—because a substantial share of those kidnappings will not affect the direct insurer or, obviously, the insured. This externality could put an upward pressure on the number and amount of ransoms being paid, which could lead to an upward pressure on the number of kidnappings and so on. This is what Anja Shortland, in her recent book on the K&R insurance market, calls the ransom externality.[218]

What is interesting for current purposes, however, is that Shortland documents how the reinsurance market, without help from any government, performs a cost-internalizing function of its own. Here is how it works. Virtually all K&R insurance is reinsured through Lloyd's member underwriters, known as syndicates, which are pooled together, for purposes of covering unexpectedly catastrophic losses, in the Lloyd's Corporation.[219] The Lloyd's Corporation, then, has the power to set capital requirements and underwriting standards for each of its syndicates.[220] As a result, Lloyd's is in a position to prevent any given syndicate—any given individual insurer—from getting into a habit of paying excessive amounts in ransom.[221] As Shortland puts it, "Lloyd's therefore has all the mechanisms in place to enforce a tacit agreement between competing insurers to operate in the long-term interest of the market."[222] What this means is that, when any given insurer pays what Shortland calls a "premium ransom"—or an unreasonably high ransom, taking into account all of the costs and benefits of ransom payouts—Lloyd's can step in and apply some discipline.[223] The overall effect is to ameliorate the third-party moral hazard effect on kidnap ransom payouts.[224]

---

[218] *Id.* at 171.

[219] *Id.* at 63, 175.

[220] *Id.*

[221] *Id.*

[222] *Id.*

[223] *Id.* at 176. This discipline can be severe. "If a syndicate takes on excessive risk or its business practices undermine the stability or smooth functioning of the market, it can be closed for new business and wound up." *Id.* at 175.

[224] Again, while this moves things in the direction of overall efficiency, it is still the case, of course, that insurers' interests and societal interests do not perfectly overlap. *See supra* note 194–95 and accompanying text.

Could reinsurers serve such a similar coordinating, cost-internalizing role in the ransomware insurance market? Possibly, although not likely. For one thing, the cyber insurance market is much larger than the K&R insurance market. While total annual K&R insurance premiums written in 2019 were in the range of $250 to $300 million,[225] the total premiums written for the cyber insurance market in 2019 were closer to $4.5 billion.[226] And roughly forty percent of that $4.5 billion in premiums flowed to reinsurers.[227] We have no data on how those premiums, and the accompanying risk, are apportioned among the dozens of reinsurance companies on the market. However, assuming it is spread across all of them roughly in proportion to their overall market share, coordination among the many cyber reinsurers would be considerably more difficult than it is within the K&R insurance market that is dominated by a single entity, Lloyd's of London.[228] This is not to say that the large cyber insurers and the large reinsurers could not, in theory, get together and provide some underwriting constraints on primary ransomware insurers. While there are over 100 direct-writing insurance companies in the U.S. that provide some type of cyber coverage, the bulk of the market share is provided by a handful of large firms.[229] Likewise, while there are dozens of reinsurers, the lion's share of that business is underwritten by a few very large companies.[230] The question,

---

[225] Patrick L. Brockett, Linda L. Golden, Stephan Zaparolli & Jack M. Lum, *Kidnap and Ransom Insurance: A Strategically Useful, Often Undiscussed, Marketplace Tool for International Operations*, 22 RISK MGMT. INS. REV. 421, 424 (2019).

[226] John Coletti, *Could Cyber Risk be a Growth Engine for Reinsurance?*, SWISS RE: REINSURANCE (Aug. 30, 2019), https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/cyber-reinsurance/reinsurance-a-growth-engine-for-cyber.html.

[227] *Id.*

[228] SHORTLAND, *supra* note 11, at 63 ("[C]ontrary to what an internet search for kidnap insurance appears to indicate, there is only one place where [kidnap] insurance is underwritten: Lloyd's of London.").

[229] Geraldine Grones, *Top 10 Cyber Insurance Companies in the US*, INS. BUS. MAG. (Dec. 20, 2019), https://www.insurancebusinessmag.com/us/news/cyber/top-10-cyber-insurance-companies-in-the-us-195463.aspx ("The top 10 insurers wrote 82.3% of the total US market.").

[230] *See* Jennifer Rudden, *Largest Reinsurers Worldwide 2020, By Net Premiums Written*, STATISTA (Jan. 11, 2022), https://www.statista.com/statistics/273158/largest-reinsurers-worldwide-by-net-premiums/.

however, is whether they would have some means of enforcement comparable to the tools available to Lloyd's. We are dubious.[231]

In the absence of coordination among cyber insurers and reinsurers, the other option is the U.S. government. That is, the federal government could perform a regulatory role with respect to the ransomware insurance market, seeking to discourage excessively high ransom payments from being made and encourage best practices by insurers, ransom negotiators, forensics firms, and other experts. Indeed, the framework already exists for this form of federal regulatory involvement. According to a recent advisory from the U.S. Department of Treasury, current U.S. law forbids ransom payments, or any payments, by U.S. parties (individual or organization) to certain foreign parties who are connected with countries subject to sanctions.[232] This prohibition is enforced by the Department of Treasury's Office of Foreign Assets Control ("OFAC").[233] OFAC maintains a list of "Specifically

---

[231] This would not be the first time that large U.S. property and casualty insurers, together with large reinsurance companies have gotten together to impose market discipline on the smaller insurers. *See, e.g.*, Hartford Fire Ins. Co. v. California, 509 U.S. 764 (1993) (addressing whether various "conspiracies" among U.S. insurers and foreign reinsurers to require certain changes to the standard commercial general liability insurance policy violated the Sherman Act or was instead protected by the McCarran-Ferguson Act). But we are aware of no such efforts by reinsurers to coordinate underwriting practices on the part of cyber insurers.

[232] U.S. Dep't of the Treasury's Advisory, *supra* note 25, at 3. Specifically, the Advisory provides as follows:

> Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA), U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).

Id. (citation omitted). Thus, by the terms of this advisory, any ransomware payment—which is a type of transaction—with any party on OFAC's SDN list would be prohibited by law. The statutes cited as authority for this prohibition are the Trading With the Enemy Act of 1917, 50 U.S.C. §§ 4301–41 and the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–06.

[233] U.S. Dep't of the Treasury's Advisory, *supra* note 25, at 3.

Designated Nationals and Blocked Persons" ("SDN List"), which are parties that all U.S. persons are forbidden to engage with, directly or indirectly.[234] Making a payment to one of these parties can subject the payer, as well as anyone who facilitates the payment (i.e., payer's insurer), to substantial civil or criminal penalties.[235] While a ransomware victim who is attacked by someone on OFAC's SDN List can apply for special permission (or a license) to enter into negotiations with that prohibited party, there is a "presumption of denial" of such requests.[236] OFAC further says that "companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response," should "implement a risk-based compliance program to mitigate exposure to sanctions-related violations."[237]

2. The Role of OFAC: Is Ransom Insurance Already Banned?

Does this mean that ransomware payments and ransomware insurance are already banned by U.S. sanctions law? Yes and no. On the one hand, there is definitely a prohibition on making payments to those ransomware attackers who appear on the SDN List, whether the payment comes from the victim or someone working on behalf of the victim, such as the victim's ransomware insurers.[238] On the other hand, the ban applies only to payments to parties on the forbidden SDN List.[239] Not all ransomware attackers are on that list. How comprehensive the ban is depends on how comprehensive that list is. Also, even insofar as the OFAC regulations constitute an existing ban, it is only a limited or contingent ban. Specifically, the OFAC appears to have some discretion in deciding whom to seek

---

[234] *Id. See also Specifically Designated Nationals and Blocked Person List (SDN) Human Readable Lists*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists (Apr. 11, 2022) ("As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries.").

[235] U.S. Dep't of the Treasury's Advisory, *supra* note 25, at 3.

[236] *Id.* at 5 ("[L]icense applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.").

[237] *Id.* at 3.

[238] *Id.*

[239] *Id.*

penalties against for such violations as well as in deciding whether there has been a violation at all. Third, it appears that if ransomware victims, often with the help of their insurers, cooperate with OFAC investigators—immediately bring the attack to OFAC's attention and follow their guidance about how to proceed—the risk of any penalty is minimized.[240] Indeed, there is a longstanding OFAC compliance process that insurers have been following for many years due to the application of the OFAC regulations to the K&R market.[241] Further, there is little evidence the OFAC is serious about enforcing the ban ransomware payments to listed entities, as there has not yet been a reported case of sanctions being imposed.

The practical effect of this regime, then, is a limited and contingent (and to date largely unenforced) ban on ransomware payments (by victims or insurers) to some subset of ransomware attackers, with OFAC playing the role of shadow regulator. We are not suggesting that OFAC is doing with ransomware insurance anything like what Lloyd's does with K&R insurance—providing a centralized sources of rules of conduct and a means of disciplining insurers who fail to follow best practices. OFAC itself has limited resources, many other responsibilities, [242] and—to date—no apparent appetite for actually sanctioning parties who transact with listed ransomware attackers. Coordinating the loss-control practices of dozens of cyber insurers may just not be a high priority. But the potential is there. For example, in its recently published guidance, OFAC noted that a key to avoiding penalties is for organizations to "implement a risk-based compliance program to mitigate exposure to sanctions-related violations,"[243] and this recommendation was expressly applied to cyber insurers, digital forensics companies, and others

---

[240] Bethan Moorcraft, *Marsh Sheds Light on OFAC's Ransomware Advisory*, INS. BUS. MAG. (Nov. 18, 2020), https://www.insurancebusinessmag.com/us/news/cyber/marsh-sheds-light-on-ofacs-ransomware-advisory-239460.aspx.

[241] *Id.*

[242] "The Office of Foreign Assets Control ('OFAC') of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States." *Office of Foreign Assets Control – Sanctions Program and Information*, U.S. DEP'T OF TREASURY, https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information (last visited Apr. 12, 2022).

[243] U.S. Dep't of the Treasury's Advisory, *supra* note 25, at 3.

who participate in the "processing ransom payments."[244] Further, in its most recent guidance, OFAC has made clear that a primary mitigating factor in avoiding fines and other enforcement efforts is to engage in just the sort of pre-breach and post-breach ransomware risk-minimization that we described above—that insurers are in a good position to identify and encourage. Specifically, OFAC says:

> Meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide, will be considered a significant mitigating factor in any OFAC enforcement response. Such steps could include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, among others.[245]

Thus, OFAC is using the sanctioning power of the U.S. government to add additional impetus for all parties involved (insureds and insurers) to implement cybersecurity best practices.[246]

Further, the mere presence OFAC, and at least the possibility that it will not grant an exception to permit payments to an attacker who appears on the SDN list, creates a degree of uncertainty about insurance coverage for ransomware payments, and that uncertainty can be a useful deterrent. That is, the existence of a potential fine from OFAC, should an insurance payment be deemed to be in violation of OFAC rules, increases the likelihood that any given potential ransomware target may not ultimately have coverage. In

---

[244] *Id.*

[245] U.S. Dep't of the Treasury's Off. of Foreign Assets Control, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments 4–5 (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf, at 4-5 (footnotes omitted).

[246] The CISA's *Ransomware Guide* referred to in the OFAC's Updated Advisory contains a list of pre-breach ("ransomware prevention") and post-breach ("ransomware response") best practices. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY & MULTI-STATE INFO. SHARING & ANALYSIS CTR., RANSOMWARE GUIDE (2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

other words, even if there is an insurance policy covering ransomware attacks, one would expect that coverage to be less likely to include insurance for the ransom payment itself insofar as such a payment could potentially be deemed a violation of OFAC regulations and thus a violation of public policy.[247] Of course, the uncertainty with respect to the OFAC fines also has a downside, insofar as it undermines the risk-spreading value of the insurance to the insured and thus discourages the purchase of coverage. The key is to make sure that hackers have greater uncertainty with respect to OFAC fines than the insureds and their insurers do. Indeed, perhaps this is one function that OFAC compliance performs; allowing the insurer and insured, to maintain some certainty that they will not be fined, while not disclosing this information to the hackers.

It is possible, then, that the current regime—including the limited ban on ransomware payments to parties on the SDN list and the emerging oversight role played by OFAC—manages the ransom externality (and the single-year-policy externality) reasonably well. Perhaps the inducement from OFAC to adopt best practices in terms of cybersecurity will be enough to motivate a change in behavior. If that is so, then no additional regulatory intervention would be necessary. On this view, what would be needed is time—time for the insurance market to develop its ability to price ransomware coverage and to develop reliable standards of cyber hygiene that insurers are willing to enforce (and continuously monitor), as some insurers are already beginning to do.[248] Therefore, if one is persuaded by the argument so far, one might be tempted to say to the critics of ransomware insurance, be patient. The insurance market and the U.S. government are figuring this out, and the solution does not need to involve, for example, banning the sale of ransomware coverage across the board.

---

[247] When insurers are found to have issued an insurance policy that provides coverage in violation of clear public policy, those insurers often are able to void coverage. One example involves insurable interests. If an insurer sells a policy that provide property coverage to someone who has no insurable interest in the covered property, the coverage is voided. Jacob Loshin, *Insurance Law's Hapless Busybody: A Case Against the Insurable Interest Requirement*, 117 YALE L.J. 474, 479 (2007). Even those hackers who are not presently on the SDN list must factor in the possibility that they will be put on the list and then their targets, and any possible insurer of their targets, will face the risk of an OFAC fine.

[248] Recall the examples, cited by Cunningham and Talesh, of At-Bay and Coalition. *See supra* note 202.

In our view, however, there is a substantial likelihood that the centralizing and cost-internalizing role played by OFAC will not be enough. How likely is it, for example, that OFAC will decide to impose sanctions on a party who makes a ransom payment because they had, prior to the attack, failed to adopt recommended cybersecurity best practices?[249] Because they have not done so to date (or at least not such sanctions have not been publicly reported), the likelihood seems small. As a result, the presence of OFAC and the threat of sanctions will have little effect on parties' pre-breach cybersecurity practices. Further, even if OFAC can make a credible commitment to include cybersecurity best practices in its determination of who gets penalized, those penalties are limited to payments made to parties on the SDN list, which is only a subset of the universe of hackers. For these reasons, we still have concerns that the ransom externality could lead to precisely the extortion economy that the *ProPublica* article predicted.[250] In the next section we offer an alternative, admittedly more radical proposal as a way of sparking further discussion.

3. Another Proposal: Banning the Bad Insurance, but Encouraging the Good Insurance[251]

Here is the proposal in brief. First, Congress would enact a ban on any payments by a ransomware insurer to cover the costs of a ransom payment, whether paid to the insured or paid directly to the attacker, and whether the attacker appears on the SDN list or not. In other words, under this proposal, Congress would impose a ban on insurance coverage of ransomware payments only. Second, the ban would be accompanied by some form of federal subsidy for cyber insurance coverage for the *other* costs of ransomware attacks, including the costs of restoring the computer system as well as business interruption and liability costs. The idea behind this two-pronged approach is straightforward: both parts of the proposal—the ban and

---

[249] *See supra* note 246.

[250] Dudley, *supra* note 10.

[251] We developed this proposal independently, but after our draft was posted on SSRN the following paper, which makes a similar proposal, was brought to our attention. *See* Jan Martin Lemnitzer, *Why Cybersecurity Insurance Should be Regulated and Compulsory*, 6 J. CYBER POL'Y 118 (2021). Lemnitzer argues that small to medium sized businesses should be compelled to buy cyber insurance. *Id.* at 129. In his view, it is this segment where cyber insurance would do the most good. *Id.* In part, Lemnitzer points to the lagging cybersecurity practices of smaller entities, which has lead them to be more frequently targeted by cybercriminals. *Id.* at 125, 131.

the mandate—would work together to undermine the profitability of ransomware attacks. The ban would reduce the available resources to those who decided to pay ransoms, and the subsidy/mandate would increase available resources for those who refused to pay ransoms. Further, by undermining the profitability of ransomware as a business model, this dual approach would reduce the threat of such attacks, thereby resulting in lower costs for the program—lower cyber insurance premiums (since the risk would be lower) and, in turn, smaller federal subsidies necessary to fund the program (since the premiums would be lower).

That is the basic idea. Now let us unpack it just a bit, beginning with the ban. The ban would, again, be on insurance payments for ransom payouts in the context of ransomware. It would be backed up with substantial fines, which themselves would also be made uninsurable. We are imagining a ban at the federal level, presumably implemented through a new act of Congress. That is, we are not making the case that OFAC or the Treasury Department generally has the authority to ban ransomware insurance coverage. So far as we know, other than the ban on payments to parties on the SDN list (discussed above), this would be the first federal ban of a particular type of insurance coverage. It would not be the first ban of any sort on a type of insurance coverage. Many states in the U.S., for example, expressly prohibit liability insurance coverage for punitive damages.[252] In addition, many states disallow coverage for intentional wrongdoing.[253]

Although this proposal would ban insurance payouts to cover ransom payments, accompanied by a threat of civil or criminal penalties against insurance companies for noncompliance, it would not ban ransom payments made by the victims of the attacks themselves. The main reason for this limitation is simple: enforcing a comprehensive ban would be an administrative nightmare. Given developments in technology, it has become increasingly easy for criminals to launch a potentially devastating ransomware attack on hundreds, even thousands, of potential victims simultaneously.[254] And while the examples of successful attacks that tend to

---

[252] *See* Catherine M. Sharkey, *Revisiting the Noninsurable Costs of Accidents*, 64 MD. L. REV. 409, 427–28 (2005).

[253] *Id.* at 432.

[254] *See, e.g.*, James Rundle, Kim S. Nash & David Uberti, *As Ransomware Proliferates, Insuring for it Becomes Costly and Questioned*, WALL ST. J. (May 12, 2021, 5:30 AM), https://www.wsj.com/articles/as-ransomware-proliferates-insuring-for-it-becomes-costly-and-questioned-11620811802 ("Groups such as

generate headlines involve large ransom payouts from medium and large-sized organizations, there are also many attacks on smaller players (small businesses and individuals) who find their systems have been locked up.[255] Many smaller attacks never even get reported to the police.[256] How would the government possibly enforce a ban against so many different target individuals and organizations simultaneously?[257] This does not seem doable.

In addition, the ban under this proposal would have an exception for ransom payouts by insurers deemed necessary to protect the health or safety of an individual or group of individuals. This exception is both a moral and a practical necessity. If an attack on a U.S. hospital were to interrupt the provision of medical services, patients could be harmed or killed.[258]

DarkSide, for example, believed to be behind the hack . . . on Colonial Pipeline Co., run a franchise business, licensing their ransomware to hacker entrepreneurs and providing them with support and training . . . ."). Indeed, Chinese hackers were able to exploit a flaw in Microsoft's Exchange e-mail server to attack hundreds of businesses. Kate Conger & Sheera Frenkel, *Thousands of Microsoft Customers May Have Been Victims of Hack Tired to China*, N.Y. TIMES (Aug. 26, 2021), https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html.

[255] *See* BARRACUDA NETWORKS, INC., SPEAR PHISHING: TOP THREATS AND TRENDS 7 (2022), https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf ("[A]n average employee at a small business with less than 100 employees will receive 350% more social engineering attacks than an employee of a larger enterprise. SMBs are an attractive target for cybercriminals because collectively they have a substantial economic value and often lack security resources or expertise."); VERIZON, 2019 DATA BREACH INVESTIGATIONS REPORT 5 fig.2 (2019), https://www.verizon.com/business/resources/reports/2019/2019-data-breach-investigations-report.pdf ("43% of breaches involved small business victims.").

[256] *See* Samara Lynn & Catherine Thorbecke, *Why Ransomware Cyberattacks are on the Rise*, ABC NEWS (June 4, 2021, 5:00 AM), https://abcnews.go.com/Technology/ransomware-cyberattacks-rise/story?id=77832650; Danny Palmer, *Ransomware Victims Aren't Reporting Attacks to Police. That's Causing a Big problem*, ZDNET (Oct. 5, 2020), https://www.zdnet.com/article/ransomware-victims-arent-reporting-attacks-to-police-thats-causing-a-big-problem/.

[257] Of course, there are far fewer ransomware insurers than there are potential ransomware victims, which is why banning, or at least regulating, the ransomware insurance market might be more practical than an outright ban on all payments.

[258] *See* Kevin Poulsen & Melanie Evans, *The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: 'They Do Not Care'*, WALL ST. J. (June 10, 2021, 11:50 AM), https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215; Patrick Howell O'Neill, *Ransomware Did Not Kill a German Hospital Patient*, MIT TECH. REV. (Nov. 12, 2020), https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-

Similarly, attacks on key infrastructure facilities, pipelines, and power grids could pose risks to health and life. An infrastructure attack, for example, that took out the electrical grid of an entire region of the country would disrupt patient care in every hospital in the region—while most hospitals have generator backups, they could also be affected by the attack if the fuel supply is disrupted. In either case, if the administrators of a hacked hospital or power facility were to decide to pay the ransom rather than take the risk of injury or death that might result, and an insurance company were to facilitate that payment, it seems unlikely that the government would, or should, follow through with any serious punishment on anyone other than the hackers.[259]

One concern with having such a life/health exception is that it might actually incentivize hackers to focus on hospitals and sensitive infrastructure even more than they already do, on the theory that such targets are more likely to have insurance coverage and thus be more likely to pay—or pay more. We have three suggestions for how to respond to this perverse incentive effect of the life/health exception.

First, this effect could be lessened by obscuring that life/health exception from the outside world, especially from potential hackers. This could be done using an approach similar to the current approach used by OFAC. That is, the government would announce publicly that insurance for all ransomware payments is banned, with no exceptions, except at the discretion of the regulatory agency tasked with overseeing these transactions (such as OFAC). That agency would then be responsible for deciding if exceptions should be made in cases in which the threat to life or health warrants doing so. The key is maintaining as much secrecy or obscurity as possible about any exceptions that are granted. This would create uncertainty with the potential hackers, and that uncertainty would serve as a tax of sorts on every ransomware attacker with respect to every attack.

Second, we could make it harder for hackers to successfully attack certain classes of sensitive targets, such as hospitals and infrastructure. For example, we could make best-practice pre-breach cyber hygiene at hospitals,

---

a-german-hospital-patient/; William Ralston, *The Untold Story of a Cyberattack, a Hospital and a Dying Woman*, WIRED (Nov. 11, 2020, 12:30 PM), https://www.wired.co.uk/article/ransomware-hospital-death-germany.

[259] For a discussion of reasons why outright bans on payments of ransom (and insurance for such payments) in the kidnap context are both immoral and impractical, see Dutton & Bellish, *supra* note 32, at 328–29.

utilities, and other such sensitive locations a matter of federal mandate.[260] The idea would be to harden these targets relative to others (where the risks of attacks can more realistically be fully insured), even though we are hoping to discourage ransomware attacks on all targets. Others have proposed creating federally mandated levels of cyber security. For example, Cunningham and Talesh, in their recent detailed proposal to adopt a comprehensive federal program for dealing with the risk of catastrophic cyberattacks, suggest mandating that all purchasers of cyber insurance products be required to maintain a baseline level of cyber hygiene, to be determined jointly by the Secretary of Treasury, Cybersecurity Infrastructure Security Agency of the Department of Homeland Security (CISA) and the new National Cyber Director (NCD).[261] We are generally sympathetic to this suggestion, though it might make sense to focus such a mandate, at least initially, on the most vulnerable potential targets.[262]

Finally, as a matter of U.S. criminal enforcement and diplomatic policy, we could make clear that ransomware attacks on U.S. hospitals and infrastructure will be prosecuted vigorously, if within U.S. criminal jurisdiction, and, if outside U.S. criminal jurisdiction, will be made a top diplomatic priority. Although the U.S. government cannot stop Russian-based hackers, Russia probably can. And as the U.S. tries to figure out what line in the sand it is going to draw for Russia on ransomware, maybe the following could be it. If you do not stop any cyberattacks on our hospitals and infrastructure emanating from within your borders or from other jurisdictions under your sphere of influence, we will take sanctions to the next level.[263]

---

[260] As the OFAC encourages compliance with the CISA recommendations, an agency could mandate such compliance for hospitals and other key infrastructure. *See supra* note 246.

[261] H. Bryan Cunningham & Shauhin A. Talesh, *Uncle Sam Re: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem via Government Backstopping*, 28 CONN. INS. L.J. 1, app. A (2021).

[262] Focusing the most draconian safety mandates on the parties who are most likely to be targeted for attacks is a common strategy in the terrorism context. Think of the special security measures taken after 9/11 at all federal buildings, which were perceived to be among the most likely future targets. *See, e.g.*, U.S. DEP'T OF HOMELAND SECURITY, FEMA 430, SITE AND URBAN DESIGN FOR SECURITY: GUIDANCE AGAINST POTENTIAL TERRORIST ATTACKS (2007), https://www.fema.gov/sites/default/files/2020-08/fema430.pdf.

[263] *See, e.g.*, Dmitri Alperovitch & Matthew Rojansky, *Ransomware Attacks Won't Stop Unless Biden Keeps the Pressure on Putin*, WASH. POST (July 6, 2021,

Just as the ban on ransom coverage would undermine the profitability of the ransomware market, so too would a subsidy for ransomware coverage for the costs other than the ransom payments—specifically, for the costs of refusing to pay the ransom. Furthermore, if a ban on insuring ransom payments were enacted, then a subsidy for cyber coverage generally would almost certainly be necessary to avoid causing a massive increase in what Kenneth Abraham and Daniel Schwarcz have called the "cyber insurance gap."[264] This gap is the vast difference between the amount of cyber insurance coverage currently being sold and the true economic risk that such attacks potentially represent.[265] The problem is that eliminating the ability of insurers to pay a ransom demand would deprive them of one important tool for minimizing their own insured costs of providing ransomware coverage. That is, some ransomware attacks may prove to be so costly that it is far cheaper for the insurer to pay the ransom than to cover the other costs resulting from the attack. This is the flipside of the collective action problem that arises if we permit insurers to cover ransom payments. Sometimes the short-run, cost-minimizing strategy for a particular insurer with respect to a particular attack, is to pay the ransom. But deprived of that tool, insurers may become less willing to write cyber policies in the first instance or perhaps they would only write the coverage with even lower limits than they are now willing to provide. This would be the greatest problem for attacks that might be considered part of a proxy cyber war on the U.S. by foreign countries. Such attacks present the sort of systematic or correlated risk that insurers have normally sought to avoid covering through the use of blanket exclusions (i.e., the war exclusion).[266]

5:01 PM), https://www.washingtonpost.com/outlook/2021/07/06/ransomware-cyberattack-biden-putin/ (arguing that, if Russia does not act on Biden's requests to stop ransomware attacks, the U.S. should "hit Russia where it hurts by sanctioning its largest gas and oil companies, which are responsible for a significant portion of the Russian government's revenue."); Nahal Toosi, *Biden Wants Putin to Behave. So Why Not Go After His Money?*, POLITICO (July 27, 2021, 3:00 PM), https://www.politico.com/news/2021/07/27/russian-critics-biden-putin-relationship-500818 (arguing for going after Putin's secret wealth if he does not deliver on ransomware attacks).

[264] Abraham & Schwarcz, *supra* note 200, at 56.

[265] *Id.*

[266] *See* Adam B. Shniderman, *Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber Insurance Policies*, 129 YALE L.J.F. 64 (2019) (discussing exclusions for acts perpetrated by hostile nations). A CrowdStrike global survey

What should the subsidy for non-ransom ransomware costs look like? One possibility would be to replicate the approach used to stabilize the terrorism insurance market after 9/11. The Terrorism Risk Insurance Program ("TRIP") was created in 2002 by the enactment of the Terrorism Risk Insurance Act ("TRIA").[267] The stated goal of the program was to provide temporary stability to commercial property insurance markets in the face of fears of a possible increase in terrorist attacks on U.S. soil.[268] What it has become over time is a more-or-less permanent federal subsidy to the U.S. terrorism insurance market.[269]

There are two essential components of the program. First, there is the supply-side mandate—that is, insurers are required to offer terrorism risk coverage in many of their property and casualty lines.[270] The mandate says

---

revealed that sixty-three percent of cybersecurity experts viewed nation-states as one of the cyber criminals most likely to cause concern, up from the previous two years. CROWDSTRIKE, 2020 CROWDSTRIKE GLOBAL SECURITY ATTITUDE SURVEY 8 (2020), https://iitd.com.ua/wp-content/uploads/2021/03/global-security-attitude-survey-report-2020.pdf. China is a particular concern as tensions between the U.S. and China increase. Kevin Collier, *U.S. Accuses China of Abetting Ransomware Attack*, NBC NEWS (July 20, 2021, 6:09 AM), https://www.nbcnews.com/tech/tech-news/us-accuses-china-abetting-ransomware-attack-rcna1448. There is evidence that cyber insurers are becoming increasingly willing to invoke the war risk exclusions, even in cases in which finding the original source of the attack is difficult. *See* Cunningham & Talesh, *supra* note 261, at 19 (describing cyber insurers' more aggressive recent use of the war exclusion as a "gathering storm").

[267] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322 (2002). The program, which has been reauthorized four times (most recently in 2019), includes a mandate that all commercial property and casualty insurers offer terrorism risk insurance coverage. FED. INS. OFF., U.S. DEP'T OF THE TREASURY, REPORT ON THE EFFECTIVENESS OF THE TERRORISM RISK INSURANCE PROGRAM 5 (2020), https://home.treasury.gov/system/files/311/2020-TRIP-Effectiveness-Report.pdf (describing mandate). This mandate does not require insurers to offer the coverage at a particular price, nor it does not require that insureds purchase the coverage. *Id.* It only requires that coverage be made available. *Id.*

[268] FED. INS. OFF., *supra* note 267, at 15 n.57.

[269] TRIA, enacted originally in 2002, was renewed in 2005, 2007, 2015, and 2019. *Terrorism Risk Insurance Act (TRIA)*, NAT'L ASS'N OF INS. COMM'RS, https://content.naic.org/cipr_topics/topic_terrorism_risk_insurance_act_tria.htm (Oct. 18, 2021). The current reauthorization is set to expire in 2027. *Id.*

[270] There are a number of lines of insurance that are expressly excluded from the TRIP program, such as professional liability insurance. *See* 31 C.F.R. § 50.4(w) (2019).

nothing about the price that insurers should charge for this coverage (presumably whatever price the market can bear), and there is no mandate on the buyer's side requiring the purchase of terrorism insurance.[271] The coverage merely has to be offered.

Second, in exchange for being required to offer this coverage, insurers are able to participate in a federally funded terrorism-risk reinsurance program, sometimes referred to as the federal "backstop."[272] Because of this backstop, in the event a terrorist attack that is certified by the Secretary of Treasury, causes a very large financial hit to the insurance industry, the U.S. government will step in and bear some portion of the cost—that is, roughly eighty percent of the cost above some triggering threshold (around $200 million), with less a twenty percent individual insurer deductible, up to a cap of $100 billion.[273] Afterwards, the government is required to recoup some portion of the reinsurance it provides, and is empowered but not required to recoup the rest, through surcharges on the insurance companies over time.[274] The subsidy exists largely because of the likelihood that, in the event of a very large loss, the government will not invoke its discretionary recoupment power, and indeed, following a massive attack on the U.S. in which the country is reeling from financial losses, may not even carry through with the mandatory recoupment.

Could such a program—with a "soft" insurer-side mandate plus the promise of a federal backstop—help to reduce the cyber insurance gap, especially in a world in which there is a new ban on paying ransomware demands?[275] What has TRIP done for the terrorism insurance market? It is generally considered to have been a success, in the sense that commercial property and casualty coverage for terrorism risks have been stable and insurers have been willing and able to offer the coverage at prices that are

---

[271] FED. INS. OFF., *supra* note 267, at 3.

[272] *See, e.g., id.* at 55.

[273] BAIRD WEBEL, CONG. RSCH. SERV., R45707, TERRORISM RISK INSURANCE: OVERVIEW AND ISSUE ANALYSIS FOR THE 116TH CONGRESS 4 (2019), https://sgp.fas.org/crs/terror/R45707.pdf.

[274] *Id.* at i ("As insured losses rise above $37.5 billion, the Secretary is required to recoup a progressively reduced amount of the outlays. At some high insured loss level, which will depend on the exact distribution of losses, the Secretary would no longer be required to recoup outlays.").

[275] Cunningham and Talesh propose such an idea as part of their "Catastrophic Cyberattack Resilience Act." Cunningham & Talesh, *supra* note 261, at app. A.

not considered outrageous.[276] However, there is also evidence that, while the adoption of TRIP increased the take-up rates of terrorism coverage over time, there are still a lot of businesses (in the neighborhood of thirty-seven percent) that decline to purchase the (TRIP-subsidized) terrorism risk coverage that is offered to them.[277] What this means is that many commercial enterprises remain uninsured or underinsured for terrorism-related risks.[278]

Less than stellar take-up rates for terrorism insurance is a problem for the obvious reason that if a catastrophic series of attacks were to happen, those businesses that did not purchase terrorism coverage may find themselves in dire financial difficulty. But less than stellar take-up rates for ransomware insurance—not coverage for ransom payouts, but coverage for the other costs of such attacks—comes with an additional cost. It would undermine the credibility of public commitments not to pay ransoms, thereby undermining our attempt to disrupt the extortion economy. What can be done about this? In addition to enacting a TRIP-like program of insurer-side mandate and federal backstop, what about the introduction of a buyer-side

---

[276] *See, e.g.*, FED. INS. OFF., *supra* note 267, at 2, 82 (concluding that the program mostly meets the goals set for it).

[277] *Id.* at 28 ("Analyses by Treasury between 2005 and 2014 found that the take-up rate, when measured by the percentage of policies containing terrorism coverage, increased from 27 percent in 2003 (the first full year of the Program) to approximately 60 percent by 2006."). Others have proposed either creating a new federal cyber-attack reinsurance regime on the TRIP model or simply expanding TRIP to cover non-terrorist cyber-attacks. *See, e.g.*, Cunningham & Talesh, *supra* note 261, at 51 (proposing the "Catastrophic Cyberattack Resilience Act," which would create a federal government backstop for the "cyber insurance ecosystem."); Abraham & Schwarcz, *supra* note 200, at 65 (suggesting the possibility of "[e]xpanding federal reinsurance to apply to all cyber catastrophes, rather than just those that meet the definition of terrorism . . . ."). But the reasons these scholars give for providing a federal backstop are primarily based on the catastrophic nature of the risk of cyber-attacks. For example, as Abraham and Schwarcz correctly point out, the risk of cyber-attack, unlike almost all other insured property and casualty risk, is not geographically bounded. *Id.* at 51. Even the worst hurricanes and earthquakes, which can involve a large geographical area, are ultimately bounded by geography. Similarly, as Cunningham and Talesh rightly emphasize, the possibility that insurers will, in the event of a massive coordinated cyber-attack, invoke the war exclusions in their policies, dramatically increases the likelihood that many claims would go uncovered. Cunningham & Talesh, *supra* note 261, at 20.

[278] Take-up rates also vary greatly by region and even by city. *See* FED. INS. OFF., *supra* note 267, at 39 fig. 26 (noting Houston's take-up rate in 2019 was fifty-five percent, whereas Washington, D.C.'s was eighty-four percent).

mandate as well? That is, we could enact a requirement that businesses and nonprofits purchase cyber insurance coverage. Insurance mandates are not unheard of. State governments have long required businesses to maintain workers compensation insurance or car owners to maintain liability insurance.[279] More recently, the federal government has famously required individuals to purchase health insurance.[280] Also at the federal level, although the National Flood Insurance Program (NFIP) does not directly mandate that all homeowners purchase federal flood insurance, it does require that anyone getting a federally backed mortgage in such a zone have flood coverage.[281] However, because many banks seem to be unwilling to enforce the flood insurance mandate, only thirty percent of homes in the highest-risk flood zones carry flood insurance, notwithstanding the mandate.[282] For that reason, in order to reduce the flood insurance gap, some have proposed making that mandate more direct, along the lines of the

---

[279] Every state requires employers of a certain size to provide workers compensation coverage. *See Workers' Compensation Laws: State by State Comparison*, NAT'L FED'N OF INDEP. BUS. INC. (June 7, 2017), https://www.nfib.com/content/legal-compliance/legal/workers-compensation-laws-state-by-state-comparison-57181/. Similarly, every state has a financial responsibility law requiring drivers to carry some minimal amount of liability coverage. *See Automobile Financial Responsibility Laws by State*, Ins. Info. Inst. (July 2018), https://www.iii.org/automobile-financial-responsibility-laws-by-state.

[280] In 2010 Congress enacted the Affordable Care Act, which included the famous "individual mandate," requiring all qualifying individuals to purchase health insurance. Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010) (to be codified at 42 U.S.C. § 18091). The relevant provision states that each "applicable individual shall for each month beginning after 2013 ensure that the individual . . . is covered under minimum essential coverage for such month." 26 U.S.C. § 5000A(a) (2011). As part of the 2017 tax bill, Congress eliminated penalties for noncompliance with the Affordable Care Act's individual insurance mandate. Sarah Kliff, *Republicans Killed the Obamacare Mandate. New Data Shows It Didn't Really Matter, Upshot*, N.Y.TIMES (Sept. 21, 2010), https://www.nytimes.com/2020/09/18/upshot/obamacare-mandate-republicans.html.

[281] Howard Kunreuther, *Improving the National Flood Insurance Program*, 5 BEHAV. PUB. POL'Y 318 (2021).

[282] *Closing the Flood Insurance Gap*, UNIV. OF PENN.: RISK MGMT. & DECISION PROCESSES CTR., https://riskcenter.wharton.upenn.edu/policy-incubator/upgrading-flood-insurance/closing-the-flood-insurance-gap/ (last visited Apr. 12, 2022).

Affordable Care Act's individual mandate.[283] Making cyber insurance mandatory would similarly reduce the cyber insurance gap.[284]

Mandating the purchase of non-ransom ransomware costs would provide a number of benefits. First, closing the cyber coverage gap would discourage ransomware attacks. This is because, if the vast majority of American businesses and nonprofits are covered by federally backed cyber insurance for any harms the attackers cause, then hackers' ability to extort ransom payments would be undermined. Encouraging, even requiring, the purchase of cyber coverage for the non-ransom costs of cyberattacks would reduce the profitability of such attacks, by reducing the cost to insureds of refusing to pay a ransom. Further, if this mandate/subsidies (along with the ban) were to dramatically undermine the incentive to engage in ransomware attacks in the first place, then the price of such coverage (and the cost to the federal budget of the subsidies) would be likewise diminished. That is, because mandatory insurance for non-ransom costs of ransomware attacks, and mandatory non-insurance of the ransom, would send a credible signal that the ransom payment would not be forthcoming, the price of the coverage would be reduced.

In addition, if insurers have more at stake in the event of a continuing onslaught of ransomware attacks, they will have much greater incentive to do better at pre-breach, *ex ante* regulation of their insureds.[285] And given insurers' superior access to direct data on what works and what does not in terms of pre-breach risk reduction (data that would accrue over time as they manage more claims), they would be in a good position—perhaps even a better position than federal regulators—to identify and implement truly optimal cyber hygiene practices among their insureds. Finally, closing the cyber insurance gap would provide the risk-spreading benefits that insurance is meant to provide—spreading the costs of ransomware attacks over the broader insurance pool.

---

[283] *See supra* note 280 and accompanying text for discussion on the Affordable Care Act.

[284] Of course, any proposal to require mandatory insurance coverage would have many obstacles to overcome, including determining what the right amount of coverage to require and the precise terms of the coverage. The few attempts that have been made by governments to require cyber coverage thus far have not been particularly successful. *See* Hai Jin Park, *Incentivizing Cybersecurity Through Cyber Insurance: Benefits and Pitfalls of Mandating Cyber Insurance* (Mar. 24, 2022), at https://ssrn.com/abstract=4065565 (discussing efforts by governments of California and South Korea to implement mandatory cyber coverage.).

[285] This again is consistent with the Abraham and Schwarcz observation. *See* Abraham & Schwarcz, *supra* note 200, at 56–57, 65, 67.

There are, of course, a number of serious objections that one could raise in opposition to this idea. First, with respect to the insurer-side mandate and backstop idea, why provide such a program for cyber risk, among all the potential catastrophic risks that might benefit from such a regime? Why not create a federal pandemic risk insurance program? Or, more generally, a federal disaster risk insurance program? In fact, although these questions take us well beyond the scope of this paper, such programs might well be good ideas and for some of the same reasons suggested here: to close the insurance gaps in those areas, putting the insurance industry on the hook for a greater fraction of those losses, and thereby incentivizing them to find ways to reduce these risks, as well as providing a means of risk spreading that has advantages over counting on *ex post* government relief. But we need not make those arguments here. A reason for beginning with cyber insurance is the additional rationale of disrupting the ransomware extortion economy—to interrupt the cycle of attacks that has made the ransomware market so profitable for so many.

CONCLUSION

The problem of ransomware attacks is pervasive, growing, and likely to continue to grow for the foreseeable future. Recent hacks originating in China and Russia have made ransomware a significant political issue. Given the potentially devastating costs of being held up by ransomware hackers, that organizations have turned to insurance as a way of managing this substantial and growing risk is unsurprising. But ransomware insurance as a social practice has come under attack. Such insurance, the argument goes, is fueling a cycle of criminal activity and providing substantial funding for criminal enterprises; making the problem worse than it would otherwise be. As a result, some critics have suggested banning such insurance.

We have argued that the story of ransomware insurance is more complex than previous reports have suggested. Insurers do much more than indemnify insureds for losses, such as by paying the ransom or the cost of restoring the network. They also offer significant pre-breach services intended to reduce the risk of a successful attack or reduce the magnitude when one ultimately happens. While recent research suggests the take-up on those services from insureds is currently low, the market is still nascent, and the rising premiums for cyber insurance may give insureds a reason to take greater advantage of these services. In addition, insurers offer post-breach services designed to assist insureds in responding to a cyberattack. Those

services may help lower the overall costs of cyberattacks, by helping insureds to negotiate lower ransom payments or even to decide to refuse to make ransom payments in favor of rebuilding their networks, the costs of which are also covered under these policies.

To be sure, there are inefficiencies arising from ransomware insurance that need to be addressed. Both the single-year-policy externality and the ransom externality can lead insurers and insureds to underinvest in preventing successful ransomware attacks and to pay excessive ransoms when such attacks are successful. Thus, the best case for ransomware insurance entails intelligent regulation of the ransomware insurance market. Others have offered suggestions for such regulation, including recommending government subsidies for (and perhaps even a mandate of) multi-year cyber policies that cover the costs of ransomware attacks, with perhaps a limited ban on coverage for ransomware payments themselves. Such regulation could in theory reduce the externalities associated with ransomware coverage and help private ransomware insurance—together with the U.S. government, perhaps through the involvement of the OFAC—serve as a socially beneficial regulator of ransomware risk. Given this possibility and the clear risk-distribution benefits of ransomware insurance (especially in cases involving risk to life and limb), we conclude that it is, at the very least, too early to declare that ransomware insurance is a net negative for society. Thus, we propose a limited ban on insuring ransom payments—with exceptions for situations involving potential serious physical harm—with a government mandate that insurers provide cyber insurance and ransomware coverage for the other associated losses (e.g., the cost of restoration). That should be backstopped by a significant reinsurance market. Given the reluctance of reinsurers to take on these risks, we discuss the potential benefits of a program akin to TRIP, under which the government would reinsure for catastrophic losses with a cost-sharing mechanism between the primary insurers and the government reinsurance program. If this program alone does not result in a drastic reduction in the cyber insurance gap, we could also consider a buyer-side cyber insurance mandate.