FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

How a Government Reinsurance Program Can Accelerate Maturation of the Cyber Insurance Market

By Nick Leiserson

June 17, 2025

Foreword

The United States faces an increasingly volatile cyber threat environment that poses serious risks to national security, economic stability, and the foundations of democracy. Against this backdrop, cyber insurance has been viewed as a helpful mechanism to manage risk and incentivize the adoption of cybersecurity best practices.

Yet despite two decades of growth, the cyber insurance market remains immature. Premiums are volatile, coverage gaps persist, and insurers lack the ability to price risk accurately. Underwriting practices have marginally improved cyber hygiene, but the market continues to fall short of policymakers' expectations. Spikes in premiums and reduced coverage have driven some companies to self-insure or forgo cyber insurance altogether.

Expecting the market to self-correct in the face of unpredictable cyber threats is misguided and dangerous. Without adequate government intervention, the cyber insurance market will not mature rapidly enough to match the pace and scale of today's cyber risks.

This report offers a comprehensive road map to accelerate the development of the cyber insurance market. In particular, the paper details how, through a tailored intervention — and at no risk to the taxpayer — Congress can establish a federal reinsurance program to reduce uncertainty for carriers and stabilize the market.

The biggest problem facing the cyber insurance market is the inability of insurance companies to diversify their risk. While property insurers can guarantee they will not have to pay out all of their policies at once by maintaining a diverse portfolio of policyholders, cyber insurers cannot. By providing policies to homeowners in both Ohio and Florida, insurance providers can guarantee that not all of their policyholders will suffer hurricane damage at the same time. In cyber, geography does not matter. Company size does not matter. Industry does not matter. Because of this, insurers have a higher cost of capital compared with other lines and cannot write as many policies, leading to premium hikes and a persistent coverage gap.

A federal reinsurance program would deal with risks associated with cyber events that can generate widespread losses across multiple sectors and affect an insurer's entire business. A federal reinsurance program would lower the cost of capital, enabling insurers to write more policies and cover more companies.

Congress has created federal reinsurance programs in the past, including the Terrorism Risk Insurance Program (TRIP) to stabilize the property insurance market after 9/11. With TRIP due to be reauthorized this Congress, there is a rare window to extend government insurance into cyberspace.

Without urgent federal action, cyber threats will continue to undermine economic stability. Congress should seize the moment to empower the cyber insurance industry to deal with risk at scale. This paper provides a compelling and detailed playbook for lawmakers.

Retired Rear Adm. Mark Montgomery
Senior Director, FDD's Center on Cyber and Technology Innovation
June 17, 2025

Executive Summary

No ship is unsinkable, and no system is unhackable. An entity is never "cybersecure"; rather, cyber is an element of enterprise risk management.[1] For decades, therefore, policymakers and business leaders have heralded cyber insurance as a key tool for reducing the impact of cyberattacks.[2] Insurance helps ensure continuity. Individuals and companies can remain productive, rather than taxing government resources, if insurance helps them become whole again following a disaster.[3] Insurance can also incentivize socially desirable behavior. By linking discounts on premiums with responsible cybersecurity choices, insurers exert pressure on policyholders to act in less risky ways.[4] Competition among insurers and their pricing models can lead to innovations in the understanding of what constitutes risky behavior.[5]

For these reasons, insurance has been around for millennia. In antiquity, "bottomry" loans for merchant ships were forgiven should the ship sink or be captured by pirates. Roman legionnaires pooled assets in burial funds to ensure those who died in the line of duty would have the appropriate funerary rites to appease the gods.[6] Risk transfer using insurance hedges against events that are predictable at a population level but unpredictable at the level of an individual or corporation. Indeed, cyber incidents happen across the economy, but there is limited or no warning of which company will be targeted.[7]

The cyber insurance market has exploded over the past 20 years. Total written premium is over $14 billion globally, the majority of which is in the United States.[8] Cyber insurers positively affect incident response by guiding their

1. U.S. Department of Commerce, National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," February 26, 2024. (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)
2. U.S. Executive Office of the President, "The National Strategy to Secure Cyberspace," February 2003. (https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf)
3. Kai-Uwe Schanz, "The Role of Insurance in Promoting Social Sustainability," *The Geneva Association*, November 2022. (https://www.genevaassociation.org/sites/default/files/2022-11/social_sustainability_report.pdf)
4. Yu-Hung Chen and Baojun Jiang, "Effects of Monitoring Technology on the Insurance Market," *Production and Operations Management*, August 1, 2019. (https://doi.org/10.1111/poms.13023)
5. The increasing use of satellite imagery for property insurance is an example of new data being incorporated into risk pricing. Alex Clere, "Earth Observation and Imaging in Insurance Underwriting," *InsurTech Digital*, December 1, 2023. (https://insurtechdigital.com/articles/earth-observation-and-imaging-in-insurance-underwriting)
6. Dan Wang, "How Maritime Insurance Helped Build Ancient Rome," *Flexport*, January 29, 2016. (https://www.flexport.com/blog/maritime-insurance-in-ancient-rome)
7. Ariel Levite, Scott Kanry, and Wyatt Hoffman, "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance," *Carnegie Endowment for International Peace*, November 7, 2018. (https://carnegieendowment.org/research/2018/11/addressing-the-private-sector-cybersecurity-predicament-the-indispensable-role-of-insurance)
8. Andreas Schmitt and Greg Eskins, "Closing the Cyber Risk Protection Gap," *Marsh McLennan and Zurich Insurance Group*, September 26, 2024. (https://www.marshmclennan.com/web-assets/insights/publications/2024/september/mmc-zurich-cyber-whitepaper.pdf)

policyholders through a breach.[9] Underwriting is beginning to yield measurable improvements in cybersecurity practices.[10] Chief information security officers report that when talking to their boards and other senior executives, underwriting conversations can provide them significant leverage to implement stronger cybersecurity measures.[11]

Yet despite its massive growth over the past two decades, cyber insurance is not living up to policymakers' expectations. There is a significant coverage gap. Most damage caused by malicious cyber actors is not insured. The market remains immature, with significant year-over-year fluctuations in premiums, contracts, and underwriting. Cyber risk pricing remains nascent, and lessons from this market-driven approach have not filtered into broader cyber policy conversations or cybersecurity operational activities.

Policymakers' hopes for cyber insurance can still be realized, but waiting for the industry to build a more robust actuarial record of claims data will take decades. This paper will explore the current condition of cyber insurance in the United States and propose how lawmakers can accelerate this market's maturation.

It will begin by identifying the challenges facing the cyber insurance market that have prevented it from meeting policymakers' expectations. The analysis will delve into supply-side constraints on the market, primarily driven by the difficulty of calculating cyber risk, that limit the ability of cyber insurers to deploy capital effectively relative to other forms of insurance. The paper will also review demand-side challenges, including unattractive policies proffered by carriers and minimal contractual requirements for insurance coverage.

This paper will then propose a solution to enhance the cyber insurance market's maturity: The U.S. government should act as a reinsurer. Congress should take the lead in establishing a limited-scope reinsurance program that would alleviate the risks and uncertainties facing cyber insurers. This discussion will outline how a reinsurance program should be set up and highlight its benefits. Reinsurance will reduce the cost of capital, lower premiums, and increase take-up of cyber insurance products. With a properly designed recoupment mechanism, these benefits can be realized at virtually no cost to the taxpayer.

Finally, the paper will chart a path forward for lawmakers to implement the proposed reinsurance program. The Terrorism Risk Insurance Program (TRIP), established in the aftermath of the 9/11 terrorist attacks, offers a helpful model, even as it differs in key ways from the proposed cyber reinsurance program. With TRIP set to expire in 2027, Congress should use its reauthorization as an opportunity to set up this needed backstop to the cyber insurance market. Doing so will materially improve the nation's cybersecurity posture at a time when the threats arrayed against America are more potent than ever.

Recommendation: Congress Should Enact a Separate Cyber Reinsurance Program as Part of the Terrorism Risk Insurance Act Reauthorization. Congress should craft and authorize a reinsurance program designed to mitigate systemic risk associated with cyber incidents that are already covered by most cyber insurance policies. The program should provide for government coinsurance above a certain threshold, have a cap on total liability, and be funded through recoupment should it be triggered.

9. Shauhin A. Talesh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses," *Cambridge University Press*, December 27, 2018. (https://doi.org/10.1111/lsi.12303)

10. "Using Data to Prioritize Cybersecurity Investments," *Marsh McLennan*, April 11, 2023. (https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Using_data_to_prioritize_cybersecurity_investments_report.pdf)

11. Stephen Lawton, "Why CISOs Should Get Involved With Cyber Insurance Negotiation," *Dark Reading*, July 27, 2023. (https://www.darkreading.com/cyber-risk/why-cisos-should-get-involved-with-cyber-insurance-negotiation)

The Present State of the Cyber Insurance Market

To accelerate the maturation of the cyber insurance market, one must understand why it has failed to meet the hopes of policymakers and why it is struggling to develop at a pace that adequately keeps up with cyber risk. Specifically, one must examine supply- and demand-side market constraints, including difficulties with risk calculation and unattractive policy options that are turning away prospective policyholders. One should also beware of counterproductive interventions in the market that policymakers should avoid.

A Failure to Meet Expectations

The growth of the cyber insurance market has stalled after a period of impressive gains. In 2021-2022, the global total written premium doubled from roughly $6.5 billion to $13.9 billion. In 2023, however, the growth rate declined to under 4 percent.[12] In the United States, statutory direct written premiums[13] declined for the first time.[14]

Despite hopes that insurance would cover most cyber losses, a persistent coverage gap remains. In one of the more rigorous assessments of the cost of cyber incidents to the U.S. economy, the White House Council of Economic Advisers estimated that cyber losses amounted to between $57 billion and $109 billion per year in 2016;[15] however, insurance claims in the United States were only about $3 billion in 2023.[16]

Despite hopes that rigorous underwriting would stimulate pro-cybersecurity behaviors, insurers have not held policyholders accountable. Underwriting, the process by which insurers assess risk and determine coverage terms and pricing, is more sophisticated today than it was a decade ago,[17] when it often consisted of questionnaires or phone call interviews.[18] This type of self-attestation has limited value for a variety of reasons, including that a company's policies and technologies are constantly changing and that modern information systems are enormously complex.[19] Moreover, the lack of significant claims adjustment — when carriers evaluate and settle insurance claims — is limiting the degree to which underwriting changes behavior.

12. "Reality Check on the Future of the Cyber Insurance Market," *Swiss Re*, November 18, 2024. (https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html); "Cyber Insurance Rates Fall as Businesses Improve Security, Report Says," *Reuters*, July 1, 2024. (https://www.reuters.com/technology/cybersecurity/cyber-insurance-rates-fall-businesses-improve-security-report-says-2024-06-30)

13. "Statutory" premiums refer to accounting practices prescribed by law. "Direct written" premiums include all the premiums received by carriers without accounting for any ceded to reinsurers. See: "Statutory Accounting Principles," *National Association of Insurance Commissioners (NAIC)*, accessed May 8, 2025. (https://content.naic.org/insurance-topics/statutory-accounting-principles)

14. "U.S. Cyber Insurance Maintains Strong Profits; Premium Growth Slows," *Fitch Ratings*, April 16, 2024. (https://www.fitchratings.com/research/insurance/us-cyber-insurance-maintains-strong-profits-premium-growth-slows-16-04-2024)

15. U.S. Executive Office of the President, Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018. (https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf)

16. The $3 billion figure is for domestic insurers, which represent about 75 percent of the U.S. market. Total covered losses are slightly higher due to alien insurers but well below estimated losses. See: Craig Kerman, Raymond Clouse, Brienna Reese, and Xuan Lin, "U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance," *AON*, August 2024. (https://www.aon.com/getmedia/4afa8654-6534-48c3-91c1-b27d57170cdb/20240806-US-Cyber-Market-Update.pdfß)

17. "Report on the Cyber Insurance Market," *National Association of Insurance Commissioners*, October 18, 2022. (https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf)

18. Ben Beeson, "Examining the Evolving Cyber Insurance Marketplace," *Testimony before the Senate Committee on Commerce, Science, and Transportation*, March 19, 2015. (https://www.commerce.senate.gov/services/files/68D2A98E-BA98-4ACA-A034-503D67AB6604)

19. Brett Helm, "Reliance on Self-Attestation Is Not Working for the Cyber Insurance Industry," *CPO Magazine*, October 27, 2023. (https://www.cpomagazine.com/cyber-security/reliance-on-self-attestation-is-not-working-for-the-cyber-insurance-industry)

Claims adjustment provides an opportunity for carriers to assess and modify coverage based on whether a policyholder lived up to commitments made during underwriting. Whether for fear of losing market share or fear of losing in court, carriers have not used this process to hold policyholders accountable for risk-mitigation procedures they claim to have implemented.[20]

Most ambitiously, policymakers hoped cyber insurance would serve as the foundation for evidence-based cybersecurity. Yet empirically backed cybersecurity controls remain few and far between.[21] Insurers and brokers are just beginning to perform more rigorous analysis tying claims data to underwriting — that is, identifying whether companies hit by cybersecurity incidents had or did not have certain protections in place.[22] Even these limited models, however, have not produced significant benefits to the broader cybersecurity community.

Policymakers, however, are not wrong to continue to hope for more from the cyber insurance market.[23] Ten years ago, there were positive trends similar to ones we see today: underwriting was being taken more seriously, actuarial data were being analyzed, and policyholders were finding utility in the product.[24] Yet, 10 years on, while progress has been made, none of the dreams has been realized.

It Will Take Too Long for the Market to Fix Itself

In response to market signals, insurers and policyholders are gradually adjusting their behavior. Yet on its own, this evolution is not happening nearly fast enough for the market to satisfy policymakers' aspirations.

Following an explosion of ransomware-related claims in the late 2010s, the insurance market hardened, driving more rigorous underwriting and increased premiums. This improved insurers' loss ratios[25] — the proportion of their premium paid out in claims — some of which had broken 100 percent,[26] but it made their products less attractive. For market growth to continue, insurers may need to soften their terms. This type of cycle is not unusual, and it should not concern policymakers *so long as underwriting standards do not slide back all the way to 2015 levels*. And there is no reason to believe they will since insurers now have experience and actuarial data tied to ransomware.[27]

20. Daniel W. Woods, "Where Are the Insurance Disputes over Cyber Hygiene?" *DanielWoods.info (blog)*, March 6, 2024. (https://www.danielwoods.info/blog/2024/cyber-hygiene-exclusions)
21. Jay Heiser, "Stop Performing Cybersecurity Theater: It Is No Longer Scaling," *Gartner Research*, January 5, 2023. (https://emt.gartnerweb.com/ngw/globalassets/en/doc/documents/779000-stop-performing-cybersecurity-theater.pdf)
22. "Using Data to Prioritize Cybersecurity Investments," *Marsh McLennan*, April 11, 2023. (https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Using_data_to_prioritize_cybersecurity_investments_report.pdf)
23. For more on challenges with the market, see: Josephine Wolff, "Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks," *The MIT Press*, 2022. (https://doi.org/10.7551/mitpress/13665.001.0001)
24. Catherine Mulligan, "Examining the Evolving Cyber Insurance Marketplace," *Testimony before the U.S. Senate Commerce Committee, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security*, March 19, 2015. (https://www.commerce.senate.gov/services/files/084D8B14-E007-48E4-953B-65219B888B2E)
25. Ben Dyson and Noor Ul Ain Adeel, "US Cyber Insurance Growth Stalls as Threats Ramp Up," *S&P Global*, May 20, 2024. (https://www.spglobal.com/market-intelligence/en/news-insights/articles/2024/5/us-cyber-insurance-growth-stalls-as-threats-ramp-up-81664841)
26. Craig Kerman, Raymond Clouse, Brienna Reese, and Xuan Lin, "U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance," *AON*, August 2024. (https://www.aon.com/getmedia/4afa8654-6534-48c3-91c1-b27d57170cdb/20240806-US-Cyber-Market-Update.pdfß)
27. Despite the softening market, brokers note that "underwriting scrutiny continues." "Q4 2024 Update on the US Cyber Insurance Market," *Marsh*, December 13, 2024. (https://www.marsh.com/en/services/cyber-risk/insights/cyber-market-update-q4-2024.html)

The accumulation of such historical claims data can drive the improvement of cyber insurers' risk models.[28] Yet progress may take decades, and waiting is not a very satisfying answer to leaders charged with improving our cybersecurity posture in the face of a dizzying array of threats.[29] Nor is it helpful to American businesses, especially small- and medium-sized ones, and nonprofits, which can face truly existential threats from cyber actors.[30] Policymakers, then, should consider ways to *accelerate* the maturity of the cyber insurance market.

One approach is to broaden the market. Increasing the number of policyholders increases the amount of claims data available. It also increases — at least to some extent — the diversity of the pool of policyholders. Additionally, growing the market helps increase the portion of cyber losses that are covered.

Growing the size of the cyber insurance market will not, per se, lead to the other outcomes desired by policymakers. Moreover, a broader dataset cannot fully substitute for a longitudinal set of claims data; while more claims data at a point in time can help build more robust models, insurers also need to see how policyholders react to changes in the broader ecosystem that cannot be captured except over time. It is, however, worth at least exploring the existing constraints on market growth to see where policy solutions might be applicable, especially as there does not appear to be inherent downside risk to expanding the market.[31] Policymakers must understand the supply-side constraints that prevent insurers from offering the type or amount of coverage that customers want, as well as demand-side constraints that limit the interest of customers in such products.

Supply-Side Constraints

The driving force behind supply-side constraints is the challenge for insurers of effectively modeling their customers' exposure to cyber risk. The more uncertainty there is around insurers' risk modeling, the more capital must be raised per dollar underwritten.[32] Reducing the uncertainty in modeling should immediately free up capacity for carriers to write more policies using their existing capital, in addition to making it cheaper going forward.

Three different types of risk affect insurers' willingness to write policies:

- *Attritional Risk*:[33] This is the chance that underwriting models mis-price cyber risk. For example, a carrier takes on more risk than expected if a model that assumes failure to broadly deploy multifactor authentication doubles the chance of a claim when doing so, in fact, quadruples the chance of a claim.

28. Some challenges with a lack of claims data may also stem from business decisions made by carriers. Shauhin Talesh, "Cyber Insurance and Cybersecurity Policy: An Interconnected History," *Lawfare*, November 4, 2022. (https://www.lawfaremedia.org/article/cyber-insurance-and-cybersecurity-policy-interconnected-history)

29. U.S. Executive Office of the President, Office of the National Cyber Director, "2024 Report on the Cybersecurity Posture of the United States," May 2024. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf)

30. Seventy-two percent of small and medium-sized enterprises without cyber insurance report that a cyber incident could destroy their business. "Cyber Round-Up: Q2 2023," *Cowbell*, 2023. (https://cowbell.insure/wp-content/uploads/pdfs/Cowbell-Cyber-Round-Up-Q2-2023.pdf)

31. If a growing cyber insurance market is inherently risky, policymakers should already be looking at intervening given the explosive growth over the past 20 years.

32. Insurers consider some of the risks in cyberspace to be completely un-modellable. As such, their focus is on excluding them from coverage entirely, which does not affect their cost of capital. Walter Kielholz, "The Cost of Capital for Insurance Companies," *The Geneva Papers on Risk and Insurance*, January 2000. (https://link.springer.com/content/pdf/10.1111/1468-0440.00044.pdf)

33. Attritional risk is used to tie the concept to attritional losses (those that are not major). Compare insurance language related to attritional loss ratios. "Financial Results Glossary," *Lloyd's*, 2024. (https://www.lloyds.com/about-lloyds/investor-relations/financial-performance/financial-results/glossary)

- *Accumulation Risk*: This is the chance that attritional (i.e., non-catastrophic) claims are significantly less independent of one another than anticipated. From a modeling standpoint, ideally, the fact that one policyholder made a claim would have no impact on the chance that any other policyholder made a claim, but that is not always the case.[34] Such correlation can lead to an unexpected surge of claims.
- *Un-Modellable Risk*: This is the chance of something inherently un-modellable happening, such as an act of war or an act of God.

Attritional Risk — Missing Metrics

When modeling attritional cyber risk, insurers face challenges similar to those confronting others in the cybersecurity field. The cybersecurity metrics integral to risk modeling are quite immature whether viewed from the standpoint of government,[35] the cybersecurity community itself,[36] or the broader community of enterprises trying to protect their systems.[37] Not many empirical studies link cybersecurity controls — or the measurement of implementation of those controls — to actual outcomes, either within cyberspace (e.g., the compromise of a system) or in the broader business sense (e.g., the cost of downtime due to a ransomware attack).[38]

Since cybersecurity lacks solid, data-driven metrics, insurers must create their own risk models. While insurers help push the industry toward better, evidence-based practices,[39] these models are currently unproven and carry more financial risk than fully tested, actuarially sound models found in other insurance lines. If insurers had more reliable models, they could offer investors the same returns on capital with less risk, making insurance carriers a more attractive investment. Lower costs would also let insurers cover more clients with the same amount of capital or reduce prices to attract more customers.[40]

Increasing the number of policyholders would give analysts more data, which would increase the fidelity of their models. This, in turn, would help them write more policies. But some intervention in the market is necessary to accelerate this virtuous cycle.

Accumulation Risk — The Problem of Diversification

When it comes to accumulation risks, the challenges facing cyber insurers are familiar to those in other insurance lines.

34. "The pre-condition for insurance to function correctly is that the risks insured should be as uncorrelated (independent of one another) as possible." "Why Insurers Differ from Banks," *Insurance Europe*, October 2014. (https://www.insuranceeurope.eu/publications/488/why-insurers-differ-from-banks/&ved=2ahUKEwiv_oju4dKLAxUxD1kFHTZGGnk4FBAWegQIKxAB&usg=AOvVaw0dHVQa10Gfa0p5P4yP61ii)
35. Katherine Golden, "National Cyber Director Chris Inglis: We Need to Become a 'Harder Target' for Our Adversaries," *Atlantic Council*, August 4, 2021. (https://www.atlanticcouncil.org/blogs/new-atlanticist/national-cyber-director-chris-inglis-we-need-to-become-a-harder-target-for-our-adversaries)
36. Roberta (Bobbie) Stempfley and Matthew J. Butkovic, "Five Reasons the Cybersecurity Field Needs Trusted Data Sets and Meaningful Metrics," *Software Engineering Institute's Insights (blog), Carnegie Mellon University*, March 11, 2020. (https://insights.sei.cmu.edu/blog/five-reasons-the-cybersecurity-field-needs-trusted-data-sets-and-meaningful-metrics)
37. "Introducing Cyber Security Risk Quantification," *UK National Cyber Security Centre*, June 23, 2023. (https://www.ncsc.gov.uk/collection/risk-management/introducing-cyber-security-risk-quantification)
38. Stewart Scott, "Counting the Costs in Cybersecurity," *Lawfare*, October 9, 2024. (https://www.lawfaremedia.org/article/counting-the-costs-in-cybersecurity)
39. U.S. Cyberspace Solarium Commission, "United States Cyberspace Solarium Commission Report," March 11, 2020. (https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report)
40. These same dynamics would also lower the cost of reinsurance for carriers, with much the same effect.

Ideally, the probability of a random event happening that could trigger a claim would be completely uncorrelated among policyholders.[41] Where that were not the case, insurers would, at least, like to be able to model the correlation.[42] For instance, the chance of two houses in a neighborhood burning down is not completely independent. After all, there could be a wildfire or another type of significant event. However, if an insurer knows that an area is not subject to frequent wildfires and that only a small proportion of fires in cities spread, it can at least bound the correlation in some way.

Sometimes, however, the correlation cannot be bounded (or the risks are completely correlated). If one house is subject to hurricane-force winds, it is a near certainty that the neighboring house also is. In such cases, insurers can diversify their risk by marketing to policyholders that lack the characteristic (in the hurricane example, geographic proximity) that drive correlations up.[43] The chance over the course of a year that a particular house in Nebraska is hit with a tornado, another specific house in Montana burns in a wildfire, and a third house in Florida is blown away in a hurricane is extremely small.

Unfortunately, diversification for cyber insurers is much more challenging than in other insurance lines.[44] First, the properties of cyberspace essentially eliminate geography as a means of injecting diversity into a portfolio of policyholders.[45] It is just as easy to hack a computer halfway across the world as it is one across the room.

Second, the technology and services all policyholders use — and malicious actors target — are, in many cases, identical.[46] Just three operating systems dominate the market for desktop and laptop computers.[47] Three hyperscale cloud infrastructure-as-a-service providers have a commanding market share.[48] This commonality extends to businesses (and governments and nonprofits) of all sizes and across all sectors.

As a result, a vulnerability in certain software can affect an insurer's entire book of business. Millions of systems can be brought down in an instant with one replicating virus or one piece of faulty code.[49]

41. The probability of a *claim* would still be correlated in some way due to underwriting standards.

42. Peng Shi, Xiaoping Feng, and Anastasia Ivantsova, "Dependent Frequency–Severity Modeling of Insurance Claims," *Insurance: Mathematics and Economics*, September 2015. (https://www.sciencedirect.com/science/article/abs/pii/S0167668715001183)

43. "Risk Diversification," *Canadian Institute of Actuaries*, May 25, 2023. (https://www.cia-ica.ca/app/themes/wicket/custom/dl_file.php?p=36317&fid=17215)

44. Darren Pain, "Cyber Risk Accumulation: Fully Tackling the Insurability Challenge," *The Geneva Association*, November 2023. (https://www.genevaassociation.org/sites/default/files/2023-11/cyber_accumulation_report_91123.pdf)

45. This is not true for all cyber losses (e.g., differences in state regulatory environments may result in different chances of insider threats), but it is true for external cyber intrusions.

46. For an understanding of the scope of the problem, consider a microcosm within the U.S. government. Ari Schwartz, John Banghart, and Tim McGiff, "Addressing Concentration Risk in Federal IT: A Center for Cybersecurity Policy and Law Tabletop Exercise After-Action Report," *Center for Cybersecurity Policy and Law*, June 2024. (https://cdn.prod.website-files.com/660ab0cd271a25abeb800453/665a2c34ecb3eb73916dd380_CCPL_ITConventrationRisk.pdf)

47. "Desktop Operating System Market Share Worldwide – April 2025," *GlobalStats*, accessed May 8, 2025. (https://gs.statcounter.com/os-market-share/desktop/worldwide)

48. Felix Richter, "Amazon and Microsoft Stay Ahead in Global Cloud Market," *Statista*, February 27, 2025. (https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers)

49. A computer "worm" is a piece of malicious code that self-replicates, allowing it to spread rapidly throughout the ecosystem. WannaCry in 2017 is a particularly notable example. Criminal Complaint, *United States v. Park*, No. MJ 18-1479 (C.D. Cal. June 8, 2018). (https://www.justice.gov/usao-cdca/press-release/file/1091951/dl?inline=); The faulty code in the Crowdstrike case was deployed in March 2024 before being triggered by a new configuration file in July. "External Technical Root Cause Analysis — Channel File 291," *CrowdStrike*, August 6, 2024. (https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf)

Cyber insurance carriers have argued that such risk is not inherently un-modellable. Carriers can understand the reliance their policyholders have on technology and assess the probability that claims will be made against a significant portion of their policies at once.[50] But this naturally limits the total coverage they are able to write.[51] It also increases the relative risk — and therefore the cost — of their capital and reinsurance.[52]

Traditional insurance lines rely on reinsurance to address residual correlation that may not have been adequately modeled (or to protect against multiple, low-probability independent events all manifesting in the same bad year). A reinsurer has multiple insurance carrier clients. To the extent that one client has mis-modeled correlation or is suffering from two low-probability events coincidentally, the reinsurer relies on that not happening to all of their carrier policyholders. The cyber reinsurance market does exist, but carriers are ceding a significant portion of their premium to reinsurers, suggesting low risk appetites from both parties.[53]

Ultimately, it is not clear that insurers can reliably diversify their policyholders absent a significant shift in the technology ecosystem. Reinsurers themselves face the same diversification problems, no matter the group of carriers for which they write policies.

Un-Modellable Risk — Kept Off the Books

Un-modellable risk in cyber is similar to other insurance lines. While accepting accumulation risk, insurers have largely succeeded in excluding un-modellable risks such as war from the coverage they offer, thereby addressing them with respect to their business interests. A decade ago, many cyber policies lacked the same explicit exclusions that were traditional in property and casualty contracts.[54] That is changing following several high-profile incidents,[55] and consistent language regarding claims for acts of war or loss of infrastructure is now also found in cyber insurance.[56] War exclusions may still lead to litigation because there is no settled case law on what constitutes, for insurance purposes, an act of "cyber war."[57] Carriers, however, are generally confident that this catastrophic risk is sufficiently excluded so as not to pose a risk to their business.[58] As such, it does not appreciably increase their cost of capital or limit the growth of the cyber insurance market.

50. Michael Georgiou, Stephan Brunner, Ed Pocock, Tim Marshall, Aidan Flynn, Henry Skeoch, Alex Jackson, Sioned Bentley, and Tim Davy, "Cyber Realistic Disaster Scenario Development and Modelling: Triple Threat — A New Malware Model for Systemic Cyber Insurance Industry Losses," *Beazley, Gallagher Re, and Munich Re*, 2024. (https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/Whitepaper-Systemic-Cyber-Insurance-Industry-Losses.pdf/_jcr_content/renditions/original./Whitepaper-Systemic-Cyber-Insurance-Industry-Losses.pdf)

51. When cyber is a small proportion of an insurer's exposure, the impact of claims being made across all of that insurer's policies is not existential — but it will need to limit the growth of its cyber line to ensure exposure does not become so.

52. For more on implicit challenges with the cyber reinsurance market, see: Henry R. K. Skeoch and Christos Ioannidis, "The Barriers to Sustainable Risk Transfer in the Cyber-Insurance Market," *Journal of Cybersecurity*, February 20, 2024. (https://doi.org/10.1093/cybsec/tyae003)

53. Ibid.

54. Or the exclusions were not enforced if they did exist. Litigation on war exclusions following NotPetya has focused on traditional property and casualty lines, not on cyber lines of coverage.

55. Most notably, NotPetya: Sean Steinberg, Adam Stepan, and Kyle Neary, "NotPetya: A Columbia University Case Study," *Columbia University, School of International and Public Affairs*, November 2022. (https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf)

56. Tony Chaudhry, "State Backed Cyber-Attack Exclusions," *Lloyd's Market Bulletin*, August 16, 2022. (https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf)

57. For a treatment of some of the key cyber factors, see: Josephine Wolff, "How the NotPetya Attack Is Reshaping Cyber Insurance," *Brookings Institution*, December 1, 2021. (https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance)

58. Andreas Schmitt and Greg Eskins, "Closing the Cyber Risk Protection Gap," *Marsh McLennan and Zurich Insurance Group*, September 26, 2024. (https://www.marshmclennan.com/web-assets/insights/publications/2024/september/mmc-zurich-cyber-whitepaper.pdf)

Insofar as policymakers believe coverage for these excluded incidents is in society's interest, their policy intervention would need to be significant, as there is essentially no market for these policies today.

Demand-Side Constraints

While supply-side constraints on the cyber insurance market derive from uncertainty in risk calculation, demand-side challenges are grounded in insurance carriers providing less attractive policy options and the lack of contractual requirements for this type of insurance coverage.

A Better Product, Please

One clear limitation on the demand for cyber policies is that companies are increasingly finding the product unattractive.[59] In principle, as exclusions rise and limits drop, premiums should come down. The opposite has been the case, however, although preliminary data for 2024 indicate prices are coming down.[60] Facing an increasingly expensive product that provided less coverage, some policyholders opted to self-insure[61] — or simply to go without any financial recovery plan in the event of a cyber incident.[62]

In the wake of the first-ever decline in total written premiums last year, insurers are moving to alter their offerings. Many are innovating, offering novel discounts for the adoption of certain cybersecurity practices or monitoring technologies.[63] For example, one insurer offers a premium discount for the ability to access and assess cloud infrastructure used by their policyholders.[64]

It is unclear what effects these changes will have on restarting the growth of the market, but the elasticity of demand means that any public policy solution *must address the concerns of policyholders*. Savings from cheaper capital as a result of better risk modeling will need to be passed on to policyholders.

Who's Asking?

The elasticity in cyber insurance demand is also, at least in part, because coverage is not usually required. The U.S. government, for example, does not set expectations for contractors to carry cyber coverage or to have explicitly self-insured against cyber risks,[65] nor is cyber insurance required as part of a broader regulatory regime for

59. Gareth Mott, Sarah Turner, Jason R.C. Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, and Edward Cartwright, "Between a Rock and a Hard(ening) Place: Cyber Insurance in the Ransomware Era," *Computers & Security*, May 2023. (https://doi.org/10.1016/j.cose.2023.103162)
60. "Q4 2024 Update on the US Cyber Insurance Market," *Marsh*, December 13, 2024. (https://www.marsh.com/en/services/cyber-risk/insights/cyber-market-update-q4-2024.html)
61. "Report on the Cybersecurity Insurance Market," *National Association of Insurance Commissioners*, November 3, 2023. (https://content.naic.org/sites/default/files/inline-files/Final%202023%20Cyber%20Report.pdf)
62. Nathan Eddy, "Organizations Consider Self-Insurance to Manage Risk," *Dark Reading*, March 30, 2023. (https://www.darkreading.com/cyber-risk/organizations-reassess-cyber-insurance-as-self-insurance-strategies-emerge)
63. "Cyber Insurance Provides Both Carrot and Stick for Cyber Security," *Risk & Insurance*, July 11, 2024. (https://riskandinsurance.com/cyber-insurance-provides-both-carrot-and-stick-for-cyber-security)
64. "Cyber Advantage – Cowbell Connectors," *Cowbell*, accessed May 8, 2025. (https://cowbell.insure/cowbell-connectors)
65. U.S. Cyberspace Solarium Commission, "United States Cyberspace Solarium Commission Report," March 11, 2020. (https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report)

businesses or individuals.[66] Few private entities require that their counterparties have some minimum level of cyber coverage.[67]

Policymakers are beginning to articulate more directly the role of cyber insurance as a tool for risk management, which could stimulate demand. Last year, the Environmental Protection Agency released a brief guide for water utilities intended to help them understand how they could integrate cyber insurance into a broader risk management program.[68] These sorts of educational interventions can help explain the benefits of cyber insurance to small and mid-sized companies that had not previously considered purchasing a policy.

To further increase demand, policymakers could go beyond education and begin requiring certain entities to purchase minimum coverage, both to hedge against operational disruption and to ensure, through underwriting, a certain level of cybersecurity controls. This type of intervention, however, would need to account for limitations on the supply side. Failing to do so would simply drive up the price of a limited supply of coverage.

In summary, the U.S. cyber insurance market faces significant challenges as it matures. Covered claims remain disproportionately low compared with national cyber losses, highlighting the market's continued room for maturation. Underwriting, while more advanced than a decade ago, struggles with accuracy due to a lack of proven cybersecurity metrics and a lack of rigorous claims adjustments to ensure network policies are being enforced. Efforts to create evidence-based cybersecurity through insurance remain limited, as actuarial data linking security controls to incident outcomes is still underdeveloped. Additionally, market constraints on both supply and demand hinder growth; insurers face difficulties modeling cyber risks, while rising costs and narrower coverage drive potential policyholders away. Although policymakers may consider mandating coverage in government contracts, thereby expanding the market, this is not a panacea.

Policy Solution — The Government as Reinsurer

To accelerate the maturation of cyber insurance markets, the federal government should establish a reinsurance program. Federal intervention is necessary because, in the absence of sufficient actuarial data about cyber risks, the market cannot quickly develop risk models that resolve its supply- and demand-side constraints. In fact, such data may never materialize given the human element inherent to cyber incidents. Hence the need for government to stand in as reinsurer.

This section will delve into practical considerations for what a government cyber reinsurance program should look like with regard to what is covered, the mechanism by which it operates, the trigger for government cost-sharing, requirements for insurers, and how the government can recoup costs.

66. For instance, the Federal Financial Institutions Examination Council has noted that cyber insurance can be an important part of risk management, but it has declined to recommend that its members (federal financial regulators) adopt requirements for carrying coverage. Federal Financial Institutions Examination Council (FFIEC), Press Release, "FFIEC Issues Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs," April 10, 2018. (https://www.ffiec.gov/news/press-releases/2018/pr-04-10)

67. Though data on the prevalence of contractual terms are sparse, the lack of penetration among SMEs in supply chains has been widely commented on. Jack Kudale, "Sector Down: Ensuring Critical Infrastructure Resilience," *Testimony before the House Homeland Security Committee, Subcommittee on Cybersecurity and Infrastructure Protection*, June 27, 2024. (https://docs.house.gov/meetings/HM/HM08/20240627/117445/HHRG-118-HM08-Wstate-KudaleJ-20240627.pdf)

68. U.S. Environmental Protection Agency, "Cyber Insurance for Drinking Water and Wastewater Systems," October 2024. (https://www.epa.gov/system/files/documents/2024-10/cyber-insurance-final-508-101624.pdf)

Why Reinsurance?

As noted, cyber risks are inherently challenging to diversify. Nor does the government have the ability to diversify these risks. Government does, however, have an immensely greater capacity to absorb losses[69] than any private company. Furthermore, the government has unique capacity to recoup losses after an incident.

A well-designed government reinsurance program would effectively address the accumulation concerns that are weighing on market growth today. What's more, it would do so in a way that minimally disrupts existing claims, contracts, or processes. In essence, the government would be removing a portion of the tail risk — low probability, high impact events — for carriers, just as traditional reinsurance does in other lines.[70] As the aggregate cost of claims for a carrier would be (nearly) capped at a level lower than the total coverage underwritten, any particular policy would be cheaper to provide and require less capital to backstop, two key desires of policymakers. In effect, a government reinsurance program allows society to continue to reap the benefits of risk pricing by insurers without penalizing them for the unique aspects of technology and the lack of historic data on which to rely.

The idea of a government cyber reinsurance program is not novel.[71] Despite being discussed for years, however, proposals have not progressed within the U.S. Department of the Treasury or Congress, in part because of the substantial design questions that need to be answered to make such a program effective.[72]

Practical Considerations — A Starting Point

Both the legislative and executive branches will need to contribute to the design of an effective backstop. Some of that work has already begun. In response to a Government Accountability Office report[73] — and in furtherance of the 2023 National Cybersecurity Strategy[74] — the Department of the Treasury's Federal Insurance Office, the Cybersecurity and Infrastructure Security Agency, and the Office of the National Cyber Director have been convening stakeholders to discuss program design.[75]

69. In fiscal year 2020, the U.S. government's deficit was $3.1 trillion (up 200 percent over the prior year) due to the COVID-19 pandemic. U.S. Department of the Treasury, Bureau of the Fiscal Service, "Highlights of the FY 2020 Financial Report of the U.S. Government," last modified April 6, 2023. (https://www.fiscal.treasury.gov/reports-statements/financial-report/2020/results-in-brief.html)

70. Depending on the parameters of the program, more or less of the existing reinsurance market might be affected by the government backstop.

71. Robert K. Knake, "Creating a Federally Sponsored Cyber Insurance Program," *Council on Foreign Relations*, November 2016. (https://cdn.cfr.org/sites/default/files/pdf/2016/11/CyberBrief_Knake_Cyber-Insurance_OR.pdf)

72. The Department of the Treasury's Federal Insurance Office noted design questions in a summary of responses to its request for information on the need for a government intervention in the cyber insurance market. U.S. Department of the Treasury, Federal Insurance Office, "Summary of Comments on Request for Comment: Federal Insurance Response to Catastrophic Cyber Incidents," March 29, 2023. (https://home.treasury.gov/system/files/311/2023-03-27%20Presentation%20Summary%20of%20Cat%20Cyber%20RFI%20Responses.pdf)

73. U.S. Government Accountability Office, "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," June 21, 2022. (https://www.gao.gov/products/gao-22-104256)

74. U.S. Executive Office of the President, "National Cybersecurity Strategy," March 2023, pages 26-27. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

75. Volatility and Risk Institute, NYU Stern, and U.S. Department of the Treasury, Federal Insurance Office, "Catastrophic Cyber Risk and a Potential Federal Insurance Response," *Conference held at NYU Stern School of Business*, November 17, 2023. (https://www.stern.nyu.edu/experience-stern/about/departments-centers-initiatives/centers-of-research/volatility-and-risk-institute/events/past-conferences/catastrophic-cyber-risk-and-potential-federal-insurance-response); U.S. Department of the Treasury, Federal Insurance Office, "Exploring Potential Forms of a Federal Insurance Response to Catastrophic Cyber Incidents," *Roundtable held at the U.S. Department of the Treasury*, May 16, 2024. (https://home.treasury.gov/system/files/311/Agenda%20for%20May%2016%20cat%20cyber%20insurance%20conference%20%28final%20public%29.pdf)

2025 is a critical period for congressional action. This section will outline a starting point for lawmakers to design a government cyber reinsurance mechanism.

What to Cover

A critical question for a government reinsurance program is whether it covers only the types of claims underwritten today or whether it also pushes insurers to cover new risks, including risks such as war and acts of God that are likely un-modellable. Broadening coverage in that way would be a mistake. **Policymakers should focus on currently covered risks.**

A reinsurance mechanism is intended to help offload accumulation risk — that an insurer's policies are not sufficiently diverse — but diversification is simply not possible in cyber to the degree that it is in more conventional areas of risk. The government standing in as a backstop mirrors the trappings of a more conventional market.

Expanding to different risks (e.g., by limiting the "war exclusion") in insurance policies changes the nature of the intervention. Instead of the government taking what insurers believe to be a modellable risk and reducing the error bars around it,[76] the government would instead be requiring insurers to cover what they believe to be completely un-modellable. In so doing, there would be significant questions about how underwriting should be conducted. What premiums should be set when insurers have no appetite for the risk in question? What practices are adequate to protect against a nation-state attack — and what model would insurers be able to use to predict that?

If a government wants to provide protections for its citizenry against "acts of war," a more effective intervention would be for the government to act as *carrier*, not reinsurer. The government could set premiums appropriate to its assessment of society's appetite for risk, effectively raising revenues to redistribute among affected entities in the event of a war-like cyber incident. Alternatively, the government could offer support after an incident, using the General Fund to support response and recovery, similar to what would happen in the case of property damage due to a war.[77]

While, as a general matter, war and infrastructure exclusions can coexist with the goals of a backstop, there are limitations on the extent of those exclusions that should be enforced as a condition for participation. Policymakers should consider refining existing un-modellable exclusions as outlined in Jon Bateman's 2020 paper, "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions," and making them the outer limit of what can be excluded. Bateman proposes that, to qualify for the war exclusion, there must be a clear geographic boundary as well as "major combat operations" between "states or statelike entities." Bateman similarly argues that the infrastructure exclusion, traditionally applied to utility outages (e.g., electricity or telecommunications), should be triggered only if there is substantial geographic impact to an "essential service." These fixes could have substantial benefits for the market itself, including reducing friction associated with litigation following incidents.

76. For more on sources of error in modeling, see: Michael Georgiou, Stephan Brunner, Ed Pocock, Tim Marshall, Aidan Flynn, Henry Skeoch, Alex Jackson, Sioned Bentley, and Tim Davy, "Cyber Realistic Disaster Scenario Development and Modelling: Triple Threat — A New Malware Model for Systemic Cyber Insurance Industry Losses," *Beazley, Gallagher Re, and Munich Re*, 2024. (https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/Whitepaper-Systemic-Cyber-Insurance-Industry-Losses.pdf/_jcr_content/renditions/original./Whitepaper-Systemic-Cyber-Insurance-Industry-Losses.pdf)

77. Indeed, the use of the term "insurance" with respect to these un-modellable risks seems a misnomer, except insofar as the government is self-insuring to have a "rainy day fund" for a catastrophe. At least in the United States, given the lack of a constitutional or statutory balanced budget requirement, the federal government does not conventionally self-insure in this manner — and it does not do so for excluded risks in other insurance lines.

For the purposes of the backstop, the proposed war exclusion ensures that common attritional claims that may involve some state attribution are still covered.[78]

With the exception of limitations on these two exclusions, policy intervention should be minimal. Many of the desired benefits of cyber insurance come from the *attritional* coverage provided by carriers. The goal of government intervention is to facilitate the day-to-day pricing of risk — and concomitant claims — by removing one of the inhibitors of the growth of that market: the significant, but unknown, correlation between incidents affecting policyholders.

As noted in Bateman's paper, some cyber claims have been paid for acts attributed to nation-states.[79] Policymakers should strive to prevent significant backsliding in this regard, as malicious actors in the employ of foreign governments have caused some of the more costly events.[80] As a general matter, however, the goal of policymakers should not be to decrease exclusions so much as to facilitate ordinary business.

Underlying this goal is the assumption that a truly catastrophic cyber incident would be, definitionally, a warlike act. It might even be a more *likely* warlike act than, say, a missile strike on the mainland United States. The geopolitical dynamics underlying such a cyberattack — namely, that the U.S. government would respond proportionately, including with lethal force[81] — mean that insurance is probably *not* the appropriate means for addressing such risk (in the same way that property insurers do not cover missile strikes).

Limiting exclusions through congressional action, rather than through existing state-level regulatory oversight, is likely only to distort the market. If insurers collectively believe a risk is uninsurable and thus needs to be excluded, and if state regulators agree, it is likely not a day-to-day risk. If policymakers demand it be covered anyway, at best, it will raise premiums — and, at worst, it will cause carriers to opt out of the reinsurance program altogether.

Crafting the Mechanism

Policymakers should make the reinsurance mechanism as simple as possible. In other government insurance backstops, insurers have some retention. This means that after a triggering event, insurers pay some portion of claims with no government reimbursement. For claims above the retention, there is coinsurance, where the carrier pays a small proportion (e.g., 10 percent) of claims, and the government pays the balance. This simple mechanism ensures that insurers have some skin in the game. At the same time, it limits their tail losses to the retention amount plus a fraction of the total coverage they've underwritten.[82]

78. "Jon Bateman, "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions," *Carnegie Endowment for International Peace*, October 2020. (https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_-_Cyber_Insurance_-_Final.pdf)

79. The litigation with respect to NotPetya focused on conventional insurance policies that were silent on their applicability to cyber, not to cyber-specific lines.

80. Given the standardization of exclusion language following NotPetya, it seems likely that this backsliding will happen with or without government intervention.

81. This has been an explicit part of NATO's posture since 2014: Michaela Prucková, "Cyber Attacks and Article 5 – A Note on a Blurry but Consistent Position of NATO," *NATO Cooperative Cyber Defence Centre of Excellence*, accessed May 9, 2025. (https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato)

82. In the United States, the Terrorism Risk Insurance Program uses this design: Baird Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress," *Congressional Research Service*, December 27, 2019. (https://www.congress.gov/crs-product/R45707)

Policymakers could attempt to set differential retentions or coinsurance percentages based on either insurer behavior (e.g., underwriting to certain standards) or the type of trigger (e.g., a nation-state incident).[83] However, beyond increasing the complexity of the program, both design choices pose additional challenges and should be resisted. When the government substitutes its judgment for that of insurers with regard to appropriate underwriting controls, it defeats one of the principal benefits of insurance: allowing the market to price risk with direct monetary consequences for mispricing it. Tying reimbursement ratios to the type of incident, similarly, implies that insurers should be pricing risk differently based on the types of cyber threat actors. Not only is that not done today, but it is also inherently tied to something that is not within the insured's control and is not modellable, as it reflects the behavior of human adversaries.

It is beyond the scope of this paper to suggest specific retention amounts or coinsurance percentages. Given the small size of the cyber insurance market today,[84] policymakers would be better served by building flexibility into these thresholds (e.g., by allowing the Department of the Treasury to set them in regulation), rather than getting bogged down setting them *a priori* in statute. Using the deductibles and coinsurance rates from the Terrorism Risk Insurance Program (TRIP) may be a useful starting point for discussion.[85]

If there are concerns about capping the total size of the program (as is also done with TRIP),[86] policymakers could consider having its payouts capped at some multiple of the rolling average of the total written premium in the market over the past five years. A $50 billion (or more) incident would likely demand bespoke government action beyond simply relying on the insurance backstop, and it should not be considered in scope for the program.

Trigger for Action

Most consequential to a backstop's design is the trigger for government cost sharing to kick in. Unlike terrorism reinsurance programs,[87] the goal of the backstop is not to cause carriers to cover damages that they would otherwise exclude. **Rather, the goal is to provide some protection against what are essentially small-scale catastrophes that affect a wide array of policyholders but fall short of acts of war, disruptions of infrastructure, or other excluded risks.**

At the core of how policymakers should think about a "small catastrophe" is that it must be a singular incident. One or more insurers may suffer what to them feel like catastrophic losses over the course of a year simply because they have poor underwriting standards. If all of a carrier's policyholders end up filing claims for ransomware while the rest of the market sees a relatively normal year, the carrier was not pricing risk accurately — and it *should* suffer in the market to drive better risk pricing in the future.

The reinsurance program should cover a "small, catastrophic incident." Small is easiest to define as policymakers can simply consider a cap on program size. Many "larger" likely catastrophes would be excluded from coverage. As such, the backstop should already be calibrated to target the types of events that could impede market maturation.

83. As a point of comparison, consider different coinsurance rates or copayments for different medical procedures where insurers attempt to incentivize preventative care by decreasing insureds' out-of-pocket costs.
84. In 2022, cyber insurance was 1 percent of U.S. property and casualty insurance premiums: "Cyber Insurance: State of the Risk," *Insurance Information Institute*, February 2024. (https://www.iii.org/sites/default/files/docs/pdf/triple-i_state_of_the_risk_cyber_02062024.pdf)
85. The retention for TRIP today is 20 percent of premiums on eligible lines, and the coinsurance is 20 percent of claims paid above that amount.
86. Under TRIP, there is no coverage from the U.S. government above $100 billion and no requirement that insurers provide coverage for such claims.
87. "Terrorism Reinsurance," *Pool Reinsurance*, accessed May 8, 2025. (https://www.poolre.co.uk/reinsurance)

What constitutes catastrophic is more complicated. Insurers tend to use frequencies (e.g., one in 100 years, one in 250 years) as a way of categorizing hazards as particularly harmful;[88] however, the extremely limited actuarial data for cyber incidents effectively prevents the establishment of such a threshold. Adding to the difficulty is that the increasing information and communications technology attack surface[89] means the potential scope of a cyber incident is changing year to year — making the actuarial data that do exist less reliable.

As a first-order approximation, policymakers should consider setting the threshold for "catastrophic" to be some portion of total written premiums. A single cyber incident that resulted in claims equivalent to 50 percent of premiums *across the entire market* certainly seems to qualify as catastrophic.[90] Policymakers could use a larger multiplier to make it less likely the backstop would be triggered. Similar to retention amounts, the catastrophic definition would best be set through regulatory action.[91]

Defining a cyber "incident" is a much more challenging prospect. For instance, an array of hostile actors all exploited the Log4Shell vulnerability. Colloquially, however, this is referred to as a single incident.[92] Should the backstop treat it as such? What about SolarWinds, where there was a single threat actor, but the degree of success in exfiltrating data depended, in part, on the nature of the victim and the configuration of its network?[93] Or the 2021 Microsoft Exchange Server vulnerability, which was initially exploited by a small group of state-affiliated threat actors but was eventually targeted by a wide array of criminals?[94] Even WannaCry and NotPetya, two of the most widespread cyber incidents on record, both relied, in part, on the same leaked exploit.[95] Should they be considered a single incident?

It may be possible to define "cyber incident" so that it captures the nuances that cybersecurity experts and policymakers use. However, even if such an approach were possible — and there is reason to believe it may not be[96] — a better policy solution would be to rely on expert judgment in defining the left and right boundaries of a particular incident (and its associated claims). This is not without precedent in insurance. Policymakers should consider appointing a small board of cybersecurity and insurance experts for this purpose. At the petition of carriers participating in the program, the board would determine the types of claims associated with an incident for the purpose of triggering government reimbursement and identifying those eligible for such reimbursement.[97]

88. Manuela Di Mauro, "Quantifying Risk Before Disasters Occur: Hazard Information for Probabilistic Risk Assessment," *World Meteorological Organization*, November 3, 2014. (https://wmo.int/media/magazine-article/quantifying-risk-disasters-occur-hazard-information-probabilistic-risk-assessment)

89. Michael Chertoff, "Cyber Risk Is Growing. Here's How Companies Can Keep Up," *Harvard Business Review*, April 13, 2023. (https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up)

90. If "silent cyber" in traditional insurance lines were eliminated (and those policies replaced with equivalent cyber coverage), a replay of the 2017 NotPetya incident would come close to meeting the threshold.

91. The annual nature of insurance policy renewal makes a regulatory approach particularly attractive. The ability to change carriers' retention amounts — or even the size of the backstop program — is unlikely to alter investments so long as regulatory changes affect only those contracts written after the changes are finalized.

92. Ryan Naraine, "Two Years On, Log4Shell Vulnerability Still Being Exploited to Deploy Malware," *Security Week*, August 22, 2024. (https://www.securityweek.com/two-years-on-log4shell-vulnerability-still-being-exploited-to-deploy-malware)

93. Raphael Satter and Joseph Menn, "SolarWinds, Microsoft, FireEye, CrowdStrike Defend Actions in Major Hack – U.S. Senate Hearing," *Reuters*, February 23, 2021. (https://www.reuters.com/article/technology/solarwinds-microsoft-fireeye-crowdstrike-defend-actions-in-major-hack-us-idUSKBN2AN1PY)

94. "Brian Carlson, "The Microsoft Exchange Server Hack: A Timeline," *CSO*, May 6, 2021. (https://www.csoonline.com/article/570653/the-microsoft-exchange-server-hack-a-timeline.html)

95. Alex Hern, "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017," *The Guardian* (UK), December 30, 2017. (https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware)

96. The disputes that have arisen in defining what an incident is *within a particular entity* during the Cyber Incident Reporting for Critical Infrastructure Act rulemaking belie how difficult it will be to come up with a broader definition.

97. Jon Bateman, "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions," *Carnegie Endowment for International Peace*, October 2020. (https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_-_Cyber_Insurance_-_Final.pdf)

Requirements of Insurers

Given policymakers' aspiration that insurance will drive positive cybersecurity behaviors and provide a key data source for evidence-based cybersecurity, **policymakers should include data-sharing requirements on participants in the backstop**.[98] Beyond data sharing and basic administrative requirements,[99] policymakers should be very hesitant to include other criteria for participation.

Some policymakers look at requirements for insurers as a backdoor means of regulating large swaths of industry that are not directly regulated by the government.[100] In the case of cybersecurity, insurers could act as *de facto* regulators, using underwriting requirements to impose minimum security standards rather than having civil servants attempt to enforce them. This provides some benefit to the insured,[101] benefit that is not always present when a requirement is enforced through the application of a fine or other civil penalty.

However, were the government to dictate minimum underwriting standards, it would prevent insurers from pricing risk. If an insurer believes that multifactor authentication (MFA) is not as useful a control as conventional wisdom suggests,[102] the carrier should be able to reduce the weight of that factor in underwriting as much as it would like — and can get backing capital for. If this approach ends up being profitable (or not), the entire community will have learned something about the efficacy of cyber controls. If the government substitutes its judgment by saying to insurers that they *cannot* write policies for companies without MFA enabled for certain accounts, the ecosystem is robbed of this important feedback mechanism.

To that end, dictating cybersecurity requirements may cause insurers to opt out of the program altogether. Reducing tail risk is certainly an attractive "carrot" to entice participation, but if it comes at the cost of their business model, it may not be worth the carriers' while to opt in to the backstop. Policymakers should not optimize a program to the wishes of the insurance industry, but they should take into consideration how effective the program will be if insurers withhold participation.

Arguably, failing to put substantial cybersecurity requirements into policies eligible for the backstop could create a moral hazard.[103] Since the taxpayer is effectively subsidizing some of the downside risk for carriers, they may — intentionally or not — undervalue the cybersecurity controls used by their insureds. In a "small catastrophe" scenario, these carriers would, presumably, be able to keep some of their premiums even as the government paid claims for companies that might not have been able to get insurance at all, absent the backstop.

This scenario *is* concerning, and policymakers should ensure it remains at the front of mind during program design. But there is reason to believe the market itself will weed out insurers susceptible to this moral hazard.

98. For more on this topic, see this paper RAND released while this memo was undergoing final editing: Sasha Romanosky, Lloyd Dixon, R.J. Briggs, and Henry H. Willis, "Insuring Catastrophic Cyber Risk," RAND Corporation, June 9, 2025. (https://www.rand.org/pubs/research_reports/RRA3817-1.html)

99. These administrative controls, for example, will need to identify which policies are included (e.g., what constitutes a "cyber" policy?), but policymakers would do well to use as light a touch as possible, relying on existing work by traditional insurance regulators and building in flexibility to evolve as the market does.

100. Shauhin Talesh, "Cyber Insurance and Cybersecurity Policy: An Interconnected History," *Lawfare*, November 4, 2022. (https://www.lawfaremedia.org/article/cyber-insurance-and-cybersecurity-policy-interconnected-history)

101. In the form of paid claims.

102. Because, for instance, it is challenging to deploy universally and to measure adoption accurately, so malicious actors can often find an account that isn't protected even when MFA is broadly deployed.

103. Bruce Schneier and Josephine Wolff, "Building a Cyber Insurance Backstop Is Harder Than It Sounds," *Lawfare*, February 26, 2024. (https://www.lawfaremedia.org/article/building-a-cyber-insurance-backstop-is-harder-than-it-sounds)

Available evidence shows that there *does* appear to be a strong correlation between resilience to attritional losses and resilience to contagion/small catastrophe losses. Patching, network segmentation, and reliable backups, for instance, all contributed to better outcomes from NotPetya[104] — and those same controls are useful in the face of conventional ransomware as well.[105] As a result, a bad faith carrier that takes on high-risk policyholders with a view of making money from a bailout will likely fail. Long before an incident that meets the reinsurance program threshold, the carrier will have had to pay out claims caused by conventional cyber criminals feasting on their insureds' poor cyber hygiene.

There are, however, some data-sharing measures that the government should strongly consider mandating for backstop participants. Validated cyber incident data is difficult to come by. It is even harder to find such data paired with information about the control environment on the victim's systems.[106] Whether due to fears of reputational harms or lawsuits by shareholders or customers, victim organizations are quite reticent to share such data — but one of the few places they do share, at least to some extent, is with their insurers.[107]

Policymakers should take advantage of the fact that insurers already have information that could be relevant to improving evidence-based cybersecurity. To wit, as a condition of participation in the backstop, the government should require insurers to share anonymized data at regular intervals with either the government or a third party (e.g., a nonprofit). The aggregate data could then be shared with the insurers themselves, as inputs to their models, and to the broader cybersecurity community, as a vital source of information about the efficacy of controls.

This data will be most useful when information about the claims is paired with information about the cybersecurity control environment.[108] While claims are dollar denominated — and thus relatively easy to normalize — as part of the program design, the government may wish to consider a standardized set of underwriting questions about the control environment to facilitate integration of data from different carriers. *Such a questionnaire should not be taken to imply that participation in the backstop program is contingent on using any of the collected data as part of risk pricing.* Insurers should, of course, use any data they collect as they see fit. But requiring that the questions be asked and that the anonymized data be shared could significantly enhance the discipline of cybersecurity, and it should not prove too onerous a burden on insurers.

Premiums vs. Recoupment

The cyber insurance market stabilization program here has been categorized as reinsurance. In the private market, insurers cede some of their premium to reinsurers in exchange for protection. Extending this model to a government program, taxpayers should not, indefinitely, be liable for losses in the market should a "small catastrophe" occur. **Policymakers should consider a recoupment mechanism to ensure that, eventually, the program is solvent even if it is forced to pay out.**

104. Ibid.

105. "Cybersecurity Performance Goals (CPGs)," *Cybersecurity and Infrastructure Security Agency (CISA)*, accessed May 8, 2025. (https://www.cisa.gov/cybersecurity-performance-goals-cpgs)

106. Mariam Baksh, "Federal Contractors Argue Cyber Insurance Isn't a Safe Bet for Better Security," *Nextgov/FCW*, October 14, 2020. (https://www.nextgov.com/cybersecurity/2020/10/federal-contractors-argue-cyber-insurance-isnt-safe-bet-better-security/169231)

107. Daniel W. Woods, Rainer Bohme, Josephine Wolff, and Daniel Schwarcz, "Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys," *USENIX*, August 2023. (https://www.usenix.org/system/files/usenixsecurity23-woods.pdf)

108 To its credit, the industry has self-organized to begin dealing with some data-sharing challenges. However, to date, it is more focused on claims data as opposed to information about the underlying controls environment. Policymakers should consider building on these efforts as part of any data-sharing requirements. For more on industry efforts, see: "CyberAcuView," CyberAcuView, accessed June 16, 2025. (https://cyberacuview.com)

The two primary competing mechanisms for funding a government backstop are prepaid premiums[109] and postpaid recoupment. In the former case, carriers participating in the program would pay an annual fee based on the total amount of claims support they could receive. In the latter, participating carriers would be assessed a surcharge on every cyber policy they sold if the backstop ended up paying out until the industry had, collectively, paid back the government.

Both approaches have merits. Premiums allow for smoother amortization, ensuring that revenues are being collected in good times, not just in the aftermath of a crisis. Premiums can be used to pay for administrative overhead necessary to run the program (as opposed to having to rely on appropriated funds). And premiums may be more politically viable, as they both force insurers to put skin in the game and demonstrate to other stakeholders, who may be skeptical of a backstop as a potential "giveaway," that insurers are paying for de-risking.

However, the lack of actuarial data makes it very hard to set premiums accurately.[110] As such, any invocation of the backstop in the short term would almost certainly lead to a dramatic increase in premiums in a way that closely resembled recoupment. Conversely, if the backstop is not invoked in the short term, insurers will, paradoxically, be deploying capital to pay fees to the government to enable them to deploy capital more efficiently.

At least in the first decade or two of the program's existence, therefore, recoupment provides a better path forward. It provides clear reassurances to legislators, budget scorekeepers, and good government advocates that there is a mechanism for repayment while delaying the invocation of such a mechanism until there is more data.[111]

As a starting point, policymakers should consider a long repayment window with capped annual premium surcharges. One of the goals of the backstop program is to stabilize the market; rapid swings in premiums due to accelerated recoupment timelines run directly contra to that objective.[112]

Another challenge that policymakers may face stems from the voluntary nature of the backstop program. There will be some incentive for previously participating insurers to opt out of the program once recoupment begins if that would mean avoiding the premium surcharges. While that can easily be avoided contractually, it would not stop new market participants from declining to participate in the program and undercutting existing carriers on price. Policymakers could make participation mandatory following the trigger being invoked as a way to avoid this problem.

What Are the Risks?

When considering the wisdom of a reinsurance program, it is useful to consider the most likely scenarios for the program over the coming years. It is possible that aggregate cyber risk has been exaggerated. It may be that NotPetya was a clear outlier, not a harbinger of hazards to come. Despite increased attack surface, cyber losses may remain eminently manageable for companies and insurers. If so, a government backstop may never be invoked — and may not come close to being invoked. In this scenario, the creation of a backstop would simply allow the

109. Similar to market-based reinsurance premium ceding.

110. In fact, if we had a better understanding of the frequency and scale of "small catastrophes," the private reinsurance market might be able to take up a lot more of the tail risk since it would be able to set premiums.

111. Baird Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress," *Congressional Research Service*, December 27, 2019. (https://www.congress.gov/crs-product/R45707)

112. Due to procedural budget rules, TRIA is designed to contain recoupment within a 10-year budget window, so the amortization window shrinks over the life of the program. Policymakers are urged to waive such rules rather than relying on accounting arcana: the net effects on the *rolling* 10-year budget window will be the same.

country to reap the benefits of cheaper capital and lower premiums today. Beyond some small overhead of creating the program office, there is essentially no cost to the taxpayer even as the program lowers the price of insurance and helps policyholders deal with day-to-day losses.

If aggregate cyber risk is as bad or worse than predicted, the backstop will be invoked. Perhaps a core identity service is taken down for weeks or, as insurers have modeled in the past, a virulent worm spreads like wildfire across the globe.[113] Losses could eclipse those of many natural disasters. In this case, taxpayers *would* be on the hook to help reimburse insurable losses.

Yet, eventually, these taxpayer losses would be recouped through the insurance market. What's more, in the absence of such a backstop, *it is very likely the government would have to intervene in any case*. Tens of billions of dollars of damage will produce disaster declarations using traditional federal authorities (e.g., the Stafford Act).[114] The response to the COVID-19 pandemic affirmed the willingness of policymakers to subsidize business interruption losses as well (e.g., through the Paycheck Protection Program).[115]

Thus, the choice is not between a government backstop and no government intervention whatsoever. Rather, the alternative is that some money will be appropriated for damages that are not covered by cyber insurance due to the coverage gap — with no clear plan to recoup the outlays.

In sum, to this point, the paper has outlined the challenges facing the cyber insurance market and proposed a solution for policymakers in the form of a government cyber reinsurance program. The proposed reinsurance program aims to stabilize the cyber insurance market by mitigating accumulation risks and ensuring affordability. By allowing insurers to retain some financial responsibility while the government absorbs major losses beyond a set threshold, the program would support existing covered risks and exert downward pressure on premiums while freeing capital to create more market capacity. The program should include an expert board that would assess incidents on a case-by-case basis to determine eligibility for government reimbursement. While participation should not be contingent on mandated cybersecurity requirements, insurers should be required to share anonymized incident data to enhance risk modeling and improve evidence-based cybersecurity practices. To ensure long-term financial sustainability, the program should be funded through postpaid recoupment rather than prepaid premiums, allowing insurers to pay surcharges on policies after a payout. Ultimately, whether cyber risks escalate to catastrophic levels or remain manageable, the backstop would provide stability, reducing reliance on ad hoc government interventions while safeguarding both insurers and policyholders and ensuring cost recovery over time.

Legislative Implementation of the Reinsurance Program

The final part of this paper will consider how to implement this proposal. It will begin by looking to an analog — the Terrorism Risk Insurance Program (TRIP) established after 9/11 — as a comparative model. It will then argue that TRIP reauthorization provides an ideal opportunity for enacting a cyber reinsurance program.

113. J. Daffron, S. Ruffle, C. Andrew, J. Copic, K. Quantrill, A. Smith, and E. Leverett, "Bashe Attack: Global Infection by Contagious Malware," *Cambridge Centre for Risk Studies, Lloyd's of London, and Nanyang Technological University*, 2019. (https://assets.lloyds.com/assets/pdf-bashe-attack-cyrimbasheattack-finalbashe-attack/1/pdf-bashe-attack-CyRiMBasheAttack_FINALbashe-attack.pdf)
114. Elizabeth M. Webster and Bruce R. Lindsay, "Congressional Primer on Responding to and Recovering from Major Disasters and Emergencies," *Congressional Research Service*, updated June 12, 2023. (https://sgp.fas.org/crs/homesec/R41981.pdf)
115. "Paycheck Protection Program," *U.S. Small Business Administration*, accessed May 8, 2025. (https://www.sba.gov/funding-programs/loans/covid-19-relief-options/paycheck-protection-program)

TRIP as a Model ...

The United States has faced challenges with human-caused threats destabilizing insurance markets in the past and has, through government intervention, alleviated those challenges. With TRIP expiring in 2027,[116] the 119th Congress has a unique opportunity to address increasing cyber risk even as it works to update the Terrorism Risk Insurance Act (TRIA).

The parallels between the cyber insurance market and the terrorism insurance market are apparent. Both involve scalable attacks by malicious actors on domestic infrastructure. Both are inherently difficult to model due to their human-caused nature. Both lack deep pools of actuarial data to fuel models.

Following the terrorist attacks of September 11, 2001, the U.S. Congress acted to create TRIP as a temporary backstop to lubricate coverage of terrorist acts within property insurance lines. At the time, insurers were increasingly excluding terrorism from their policies, and there were concerns that this would eventually hinder the financing of large commercial real estate projects. The resulting program, which is, in many ways, similar to the backstop outlined in this paper, has gone well beyond its three-year mandate and continues to support the property and casualty market — all at minimal cost to taxpayers.[117]

Like TRIP, the cyber reinsurance program proposed here is a coinsurance model with a total cap on liabilities from the government and carriers. Like TRIP, it relies on recoupment as the mechanism to ensure taxpayers are eventually made whole. Like TRIP, it aims to leverage the existing market rather than substituting bureaucratic judgment as to the price of risk. There are, however, key distinctions between the cyber approach and the terrorism approach.

... But With Key Distinctions

TRIP is predicated on reversing an exclusion. Insurers were concerned about their ability to model terrorism risk and therefore began excluding acts of terror from their coverage. As discussed, the cyber insurance challenge is borne more of accumulation or aggregation risk — that of a "small catastrophe" — rather than excluding entire categories of coverage.

That manifests in differences in program design. TRIP *requires* every insurer to offer terrorism insurance (with its own associated premium). The scope of that coverage is also, effectively, the scope of the program. Much of the risk underlying the policies is assumed to be catastrophic, as there are very few attritional terrorist attacks.[118] Since it is mandatory to participate, recoupment covers the entire market, and because terrorism risk is viewed to be overwhelmingly catastrophic, there is no emphasis on data collection.

The biggest difference between a notional cyber insurance backstop and TRIP, though, is the state of the market at its inception. TRIA came at a time of crisis for the insurance industry; despite some headwinds, cyber insurance is not in those dire straits. Nonetheless, the time to act is now — and TRIA reauthorization provides a unique opportunity to do so.

116. Terrorism Risk Insurance Program Reauthorization Act of 2019, Pub. L. 116-94, 133 Stat. 3026. (https://www.congress.gov/116/plaws/publ94/PLAW-116publ94.pdf)
117. Baird Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress," *Congressional Research Service*, December 27, 2019. (https://crsreports.congress.gov/product/pdf/R/R45707)
118. There has been no certified terrorist attack under TRIP since the inception of the program, much less one that hit any of the loss thresholds for the reinsurance to kick in.

Do Not Miss the Opportunity for TRIA Reauthorization

TRIP expires on December 31, 2027. However, because insurance contracts are largely written on an annual basis, unless TRIA is reauthorized by December 31, *2026*, it is likely that there will be some disruption in the property and casualty market as carriers consider whether to exclude terrorist events that occur once the backstop no longer exists.[119] The 119th Congress will be under pressure to consider legislation updating and extending TRIA.

In past reauthorizations, the issue of cybersecurity has come up, particularly with respect to whether terrorist attacks that caused property damage using cyber tools would qualify for reinsurance under the law.[120] Cyber terrorism, however, is not where the bulk of the risk is for critical infrastructure in the United States.

The House Financial Services Committee and the Senate Banking Committee have the opportunity to be bold and address a weakness in the insurance market proactively. By stating their intent to examine cyber as part of a broader look at the insurance needed for human-caused incidents, the committees can take advantage of a moving legislative vehicle and its concomitant hearings and markups to develop and enact the program outlined in this paper.

Conveniently, the executive branch has also been exploring policy interventions in the cyber insurance market. In particular, the Department of the Treasury's Federal Insurance Office — the program office for TRIP — held several workshops in conjunction with the White House Office of the National Cyber Director. In 2022, the office sought information from the public on what a policy response could look like. The committees should conduct appropriate oversight of this work and, as proper, use it in refining the legislative proposal outlined in this paper.

Conclusion

Congress and the administration should not let this opportunity go to waste. TRIA was last reauthorized for eight years, and it is unlikely the banking committees will return to the intersection of national security and insurance this decade. The cyber insurance market cannot mature fast enough to help address the pace and the scale of threats. A backstop is a critical tool to accelerate that maturity while also helping the entire cybersecurity discipline to become more data driven. By acting now, lawmakers can get ahead of the curve, materially improving the U.S. cybersecurity posture and helping their constituents — not simply the insurers — deal with cyber threats.

119. A similar hiccup happened when the program wasn't reauthorized with a year to spare in the 2010s: "Policyholders Face Uncertainty After Lapse of Terrorism Risk Insurance Program," *Proskauer*, January 6, 2015. (https://www.proskauer.com/alert/policyholders-face-uncertainty-after-lapse-of-terrorism-risk-insurance-program)

120. Gregory J. May, "The TRIA Cyber Risk Coverage Debate: Should Be Resolved as Part of Its Renewal," *Nelson Mullins LLP*, accessed May 22, 2025. (https://www.nelsonmullins.com/storage/8a6a44e4523b7c75ab341dacf271523c.pdf)

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

FDD's Center on Cyber and Technology Innovation

FDD's Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats to and opportunities for national security presented by the rapidly expanding technological environment.

Nicholas Leiserson served as assistant national cyber director for cyber policy and programs at the Office of the National Cyber Director, leading efforts on critical infrastructure protection, regulatory harmonization, cyber insurance, and software liability. Prior to that, Nick spent more than a decade on the staff of Rep. James Langevin (D-RI), advising the congressman on cybersecurity issues and serving as the staff lead for the Congressional Cybersecurity Caucus. Nick is now a senior vice president for policy at the Institute for Security and Technology.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the author do not necessarily reflect the views of FDD, its staff, or its advisors.