The Geneva Papers on Risk and Insurance - Issues and Practice
https://doi.org/10.1057/s41288-025-00346-3

Insuring the "uninsurable" cyberwarfare: rethinking war exclusions in cyber policies and the role of insurance in global cybersecurity governance

Qihao He[1] · Michael Faure[2,3] · Chun-Yuan Chen[4]

Received: 27 August 2024 / Accepted: 13 February 2025

Abstract

This paper examines the insurance of cyber-related risks, concentrating on cyberattacks that fall under the war exclusion in insurance contracts. We argue that though it is understandable that insurers include war exclusions to limit their risk exposure, this seriously limits the availability of cover when it is most needed. One of the problems is that insurers do not engage as often in risk differentiation as is predicted by the theory holding that insurance is a governance system. We therefore argue that there is an important role for governments to play, similar to other major risks like natural catastrophes and terrorism where the state often acts as a reinsurer of last resort. This paper argues that a multilayered insurance arrangement with governments could play an important role in guaranteeing substantial compensation to victims in case of cyberwar, while also reasonably limiting the risk exposure of insurance companies.

✉ Chun-Yuan Chen
cyc@mail2.nccu.tw

Qihao He
qihaohe@gmail.com

Michael Faure
michael.faure@maastrichtuniversity.nl

[1] College of Comparative Law, China University of Political Science and Law, 25 Xitucheng Road, Haidian District, Beijing 100088, China

[2] METRO, Faculty of Law, Maastricht University, 6200 MD Maastricht, The Netherlands

[3] Rotterdam Institute of Law and Economics, Erasmus School of Law Rotterdam, 3062 PA Rotterdam, The Netherlands

[4] Department of Risk Management and Insurance, National ChengChi University, No. 64, Sec. 2, ZhiNan Rd., Wenshan District, Taipei City 11605, Taiwan, R.O.C.

Published online: 12 March 2025

Introduction

Cyberwarfare is one of the most dangerous threats to global security in the context of geopolitics. It also has an ambiguous status in conventional laws of war and insurance. For example, the 2017 NotPetya cyberattack, which was driven by broader political motivations, caused an incredible amount and variety of damages and legal debates globally (Wolff 2021a, b). Some insurers refused to pay NotPetya-related claims by referring to war exclusions in insurance policies (Ferland 2019). War exclusions are long-standing clauses that deny coverage for "hostile or warlike action in times of peace and war" perpetrated by states or their agents.[1] The definitions of war articulated in cyber insurance policies offer a unique perspective on the comprehension of cyberwarfare. Legal cases challenging war provisions scrutinize government-constructed narratives around warfare and aggressive cyber actions. Nonetheless, the provisions of insurance policies in these cases offer scant clarity in their definitions; instead, they incite a legal discourse wherein evidence is introduced and undergoes rigorous logical scrutiny (Woods and Weinkle 2020).

Damage resulting from cyberattacks has often been excluded from cover through such clauses that exclude risks related to warfare. On the one hand, it is understandable that insurers want to limit their risk exposure in the case of cyberwarfare. On the other hand, it is problematic that cover is not available precisely when it is most needed. This paper examines this problem. We start by focusing on the insurability of cyber risks generally, mostly from an insurance theoretical perspective. We then discuss the way in which war exclusion clauses have been applied in practice in many cases involving cyberattacks. We go on to discuss the important role of insurance, both as an instrument that provides compensation but also in providing incentives for prevention, otherwise known as insurance as governance (via risk differentiation to control moral hazard). We argue that insurers' governance efforts, particularly with respect to cyber risks, are less than could be expected. We then present our proposed solution: a multilayered insurance model where the government is the reinsurer of last resort. We argue that this can both stimulate demand for insurance cover and boost the role of insurers in mitigating cyber risks. The final section concludes.

Within this structure the article addresses the following research questions:

(1) How does cyber insurance currently function, especially with relation to the insurability challenge of cyberwarfare? (2) What are the impacts of cyber insurance on incentives for *ex ante* cyberwar-risk mitigation and international cyber governance? (3) How should governments, when necessary and as insurers of last resort, augment and support the efficient functioning of the cyber insurance market?

[1] See, for example, *Mondelez International, Inc., Plaintiff, V. Zurich American Insurance Company*, Defendant., 2018 Wl 4,941,760 (Ill.Cir.Ct.).

Insurability of cyber risks

The prerequisite for discussing underwriting or excluding cyberwarfare lies in assessing the insurability of cyber risks, since insurance has traditionally and consistently played a pivotal role in mitigating geopolitical war risks, from world wars to the maritime piracy crisis in Somalia (Cremer et al. 2024). Insurability remains a perennial topic of scholarly discussion for emerging risk categories like cybersecurity. For example, insurance economists assert that insurable risks must meet two prerequisites: firstly, the risk must be identifiable, and secondly, it must be quantifiable in terms of cost (Kunreuther 2008). Insurance lawyers highlight three components of insurable risk: the risk must be precisely evaluated, the premium must be fair, and the potential loss must be manageable (Knutsen 2021). Cyber risks are undoubtedly considered a catastrophic or even a systemic risk (for example, see Lloyd's 2015; Scheuermann 2018; Abraham and Schwarcz 2021). Through a comprehensive review of the existing literature and an examination of cyber insurance practices, we present and review four benchmarks for evaluating insurability, tailored specifically to cybersecurity risks.

Actuarial benchmark

Actuarial benchmarks assess the predictability of risk. At its core, insurance relies on a straightforward mathematical formula: the actuarially justified premium, which the insured must at a minimum contribute (inclusive of administrative costs), should equate to the probability (p) of an event occurring, multiplied by the potential damage (D) should that event materialize. Furthermore, the cumulative premiums gathered on this premise should theoretically be adequate (paired with the insurer's accumulated reserves) to offset any loss incurred in the event of an occurrence (He et al. 2023). Compared with traditional risks (e.g., fire), cybersecurity risks have a higher degree of unpredictability. With the development of network technology and the digital economy, the probability and potential damage of cyber risks are increasing and even becoming more difficult to quantify and assess. However, neither the magnitude of the risk nor the projections of potential losses have hindered the success of insurance operations in the past (Jaffe and Russell 1997). A retrospective glance at insurance's historical record reveals numerous instances of insurance coverage against catastrophic losses that insurers were unable to foresee (Baker 2008). While there may be a dearth of new risk statistics for cyber (grounded in historical loss patterns), that does not inherently render the risk uninsurable, provided the insured can conduct a risk evaluation through modeling exercises. Insurers can model risk assessment or increase risk premiums to cope with cyber uncertainty in the early stages of underwriting due to the lack of historical data. With the assistance of InsurTech, big data, and AI, cybersecurity risks will be easier to identify and quantify, thereby reducing unpredictable risk profiles.

Solvency benchmark

The solvency benchmark evaluates the potential loss in the event that the risk materializes. It defines the necessary resources and capabilities of insurers to effectively manage and mitigate losses in the event of a cyberattack. The primary challenge lies in the possibility of numerous losses occurring simultaneously, such as war or warlike actions leading to a collective accumulation that could exceed an individual insurer's capacity. To mitigate the substantial losses stemming from cyber risks, insurers could offer assessment insurance policies, enabling them to collect premiums in the event of an exhausted insurance fund (Baker 2008). Additionally, insurers could acquire external funding via reinsurance arrangements or the issuance of insurance-linked securities, thereby safeguarding themselves against catastrophic claims (Schwarcz 2022).

Moral benchmark

The moral benchmark explores the random nature of risk. The moral benchmark tests whether the insurer can control the insured's moral hazard and adverse selection for calculated risk (Lobo-Guerrero 2012). In cybersecurity, the prevention of moral hazard is technically difficult, as there is no consensus on what technologies are effective in preventing (ever-changing) cyber risks (Wolff 2022). However, the insurance as governance theory suggests that insurers have the incentives as well as the technical measures to achieve effective control over the moral hazard of the insured (Talesh 2018). Insurers can help the insured prevent cybersecurity risks at minimal cost by imposing *ex ante* safety measures. More importantly, insurers can achieve risk control through process management, such as procuring the services of third-party cybersecurity organizations, guiding and supervising the behavior of insureds through market-based means, and reducing risks such as data leakage, thus establishing an effective cybersecurity risk protection and governance mechanism (Herr 2021). Insurance could even create moral opportunity which is, "the opportunity to cooperate with and help others," supported by "motives of charity, compassion, civic responsibility, and justice." (Elliott 2021). Through its impact on political culture and collective political action, insurance broadens our understanding of what we consider adverse and worthy of collective responsibility, thereby generating social benefits (Elliott 2021, pp. 210–212).

Economic benchmark

The economic benchmark (through the supply–demand framework) measures the willingness of insurers and insureds. From the supply side, insurers face a number of challenges in providing cybersecurity insurance products, such as catastrophe losses due to systemic and correlated risks, lack of risk and loss data, and untested policy terms and conditions in court. Moreover, some standalone cybersecurity insurance products are vulnerable and unstable due to their lack of

reliance on comprehensive risk modeling or risk-based data (French 2021). On the demand side, insufficient demand from policyholders stems from the cognitive bias that cybersecurity attacks "won't happen to me" or the mistaken belief that traditional insurance inherently covers cyber risks. Furthermore, the high cost of premiums leads to a significant imbalance in risk assessment for insured parties, disrupting the supply–demand equilibrium (Lior 2022). Despite these challenges, potential demand for cybersecurity insurance remains substantial due to the non-eliminable nature of cyber risks and increasing administrative regulations and civil liabilities (Munich Re 2023).

In summary, insurability is not a binary concept (i.e., a risk is either insurable or uninsurable) but rather an evolving one. The boundaries of insurability for a given risk are not fixed. For instance, traditional uninsurable risks such as terrorist attacks and natural disasters are now partially or even fully covered by insurers (with government support). Despite the unique nature of cyber risks, and acknowledging that there may be gaps in meeting some criteria (e.g., solvency benchmarks might require government support), it is still possible to conclude they largely meet the requirements for insurability. In practice, however, some insurers decline to cover cybersecurity hazards, citing their uninsurable nature, and argue that the insurability, availability, and affordability of cybersecurity insurance can only be achieved with government backing (US Department of the Treasury 2016). For example, a case study in the Netherlands offers insight into how insurance firms craft their contracts and tackle insurability obstacles for cyber risks, such as their interconnectedness and the scarcity of actuarial data in this specialized area (Nieuwesteeg et al. 2018). An investigation into the German small- and medium-sized enterprise (SME) cyber insurance market also reveals the challenges insurers face in addressing the substantial accumulation and unpredictability of these risks. Cyber insurance experts from various areas of the industry concur that the risk of cyber warfare is presently uninsurable, stemming from its extensive incalculability and unquantifiable nature (Cremer et al. 2024). There is even a distinction between "normal" cybersecurity risks, which are (conditionally) largely insurable, and "cyber warfare," which is still considered largely uninsurable. Of course, drawing a line between these may often be difficult. In the subsequent section, we delve into the legal disputes and the insurability of damages arising from cyber warfare and explain why insurers opt to retreat from this specialized market, leaving businesses and organizations exposed to the financial consequences of cyber warfare attacks.

Cyber war exclusion litigation and insurance clause interpretation

This section reviews the evolution and interpretation of war clauses in litigation so insurers can better quantify and control the costs resulting from offensive cyber operations, which enables insurers to describe the circumstances in which cyber war or warlike actions are uninsurable.

War exclusion clause

The purpose of a war-risk exclusion clause is risk management, primarily by excluding risks that are difficult or impossible for insurers to assess accurately.[2] A standard war-risk exclusion clause defines an act of war as any action by a government or sovereign power, its military, naval, or air forces, or by an agent acting on behalf of such government or power. This action must be characterized as "hostile" or "warlike," and the involvement of a governmental body or association is typically a prerequisite (Patel 2021).

Previous cases have demonstrated that courts often adopt a conservative approach when interpreting exclusion clauses related to war. The philosophy is relatively simple: an exclusion clause should be interpreted narrowly. If cyber risks are therefore not explicitly excluded, courts tend to assume that they are included in the insurance cover. Several examples illustrate this point:

Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co.

Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co. stands out as a prominent case in this regard, particularly for determining whether an action qualifies as hostile or warlike. On September 6, 1970, Pan American Flight 083 was hijacked by Popular Front for the Liberation of Palestine (PFLP). The Boeing 747 aircraft was flown to Egypt while still under PFLP control. Subsequently, it was completely destroyed after the passengers had been evacuated.[3] The Court upheld the district court's decision, sharing their interpretation of the all-risk exclusions. Terms such as "military… or usurped power," "war," "insurrection," and others in the two policies did not encompass a hijacking by two individuals in this case. The control of territory was subject to the Jordanian government's tolerance, and was thus insufficient to qualify as a military or usurped power. As a result, the war exclusion did not apply. Additionally, there was no significant indication of the PFLP's intent to participate in a war in the Middle East or an insurrection in Jordan. Since hijacking was not specifically excluded, and the principle of contra proferentem was applied, the judge ultimately affirmed the district court's decision.

Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co.

In 2014, following Hamas's rocket attacks from Gaza into Israel, plaintiffs Universal Cable Productions, LLC, and Northern Entertainment Productions, LLC, relocated their television production operations out of Jerusalem due to the escalating hostilities. This relocation incurred significant expenses, leading the plaintiffs to file

[2] § 13:30. Exclusions (general liability)—War-risk exclusions, Practical Tools for Handling Insurance Cases 2: § 13:30.

[3] *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co.*, No. 73-2604, 1974 WL 61146 (2d Cir. Oct. 15, 1974).

an insurance claim under their television production insurance policy. However, the policy contained war exclusions, which specifically excluded coverage for expenses resulting from "war," "warlike action by a military force," or "insurrection, rebellion, [or] revolution." The insurer, defendant Atlantic Specialty Insurance Company, denied coverage, asserting that while the policy covered expenses related to terrorism, it excluded coverage for damages arising from hostilities. Hamas's actions were considered acts of war, falling under the excluded category, and thus were not covered.[4]

The Court applied the rule "The burden is on the insured to establish that the claim is within the basic scope of coverage and on the insurer to establish that the claim is specifically excluded."[5] Since the plaintiff showed primary insurance coverage, the burden shifted to the insurer to prove that the action was properly excluded (Chopra 2021). The plaintiffs also showed that "war" required hostilities between de jure and de facto governments, and the organization known for violence was not de jure or de facto a sovereign. Therefore, terrorism by that organization could not be defined as "war" or "warlike action by a military force" in exclusions.

Holiday Inns Inc. v. Aetna Ins. Co.

In *Holiday Inns Inc. v. Aetna Ins. Co.*, plaintiffs Holiday Inns, Inc. and Holiday Inns, Inc. filed suits against Aetna Insurance Company for insurance coverage, because the plaintiffs' hotel in Beirut, Lebanon was severely damaged. The defendant argued that such damages fell under the excluded peril of insurrection, civil war, or war. The court ruled that merely claiming to be a "de facto government" or a "quasi-sovereign entity" is inadequate to attain recognition. It emphasized that for a group or entity to be considered as such, it must control territory within the boundaries of a sovereign state with the explicit consent of that state's de jure government. Even if the P.L.O./Palestinians in Lebanon was regarded as a quasi-sovereign entity, there is no indication that they were engaged in hostilities with another recognized governmental entity that resulted in or contributed to the damage inflicted upon the Holiday Inn.[6] The Court followed *Pan Am. World Airways, Inc.* in construing the war exclusion more conservatively. As a result, the war exclusion did not apply.

[4] *Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co.*, 929 F.3d 1143, 1147 (9th Cir. 2019).

[5] *MacKinnon v. Truck Ins. Exch.*, 31 Cal.4th 635, 3 Cal.Rptr.3d 228, 73 P.3d 1205, 1213 (2003). *Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co.*, 929 F.3d 1143, 1151 (9th Cir. 2019).

[6] *Holiday Inns Inc. v. Aetna Ins. Co.*, No. 77 CIV. 2623-CSH, 1983 WL 1003788 (S.D.N.Y. Sept. 19, 1983).

War exclusion in the field of cyber risk

Mondelēz International, Inc., Plaintiff, V. Zurich American Insurance Company

Mondelēz International, Inc. manufactures and markets snacks and beverage products, and is ranked as one of the largest snack companies in the world. Mondelēz purchased property insurance form Zurich, insuring "all risks of physical loss or damage" to the property and including "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction…."[7] In 2017, Mondelēz suffered a loss caused by NotPetya malware. Zurich denied the claim, because the damage was caused by a "hostile or warlike action in time of peace or war." In the end, Zurich settled with Mondelez in 2022. Even though the settlement left looming questions on attribution for cyberwar-like acts, it probably implied that the court was beginning to weigh in favor of Mondelez. Thus, Zurich had incentives to wrap things up, while there was still room for negotiation (CSO 2024; Reinsurance News 2024).

Merck & Co., Inc. v. ACE Am. Ins. Co., et al.

In 2017, Merck's computer systems were infected by the NotPetya malware. Damages were caused to 40,000 computers and losses amounted to USD 1.4 billion. Merck had all-risk insurance with ACE, covering loss or damage resulting from the destruction or corruption of computer data and software.[8] However, ACE denied coverage, arguing that the NotPetya malware was attributed to hostilities by the Russian Federation against Ukraine. Consequently, based on the war exclusion clause in the policy, such damages were deemed ineligible for coverage.[9] Merck contended that this exclusion only pertained to conventional forms of warfare and not to malware attacks. The court reviewed the ordinary meaning of exclusions, demonstrating that "warlike" could only be interpreted as "similar to war" and "related to or characteristic of an enemy; related to or engaged in actual hostilities."[10] Even though ACE had the ability to specifically and more clearly exclude cyberattacks and make

[7] *Mondelez International, Inc., Plaintiff, V. Zurich American Insurance Company*, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.).

[8] *Merck & Co., Inc. v. Ace American Ins. Co.*, 2022 WL 951154, at *1 (N.J.Super.L.).

[9] "A. 1) Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack: 2 a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval, or air forces; b) or by military, naval, or air forces; c) or by an agent of such government, power, authority or forces; This policy does not insure against loss or damage caused by or resulting from Exclusions A., B., or C., regardless of any other cause or event contributing concurrently or in any other sequence to the loss." *Merck & Co., Inc. v. Ace American Ins. Co.*, 2022 WL 951154, at *1–2 (N.J.Super.L.).

[10] *Merck & Co., Inc. v. Ace American Ins. Co.*, 2022 WL 951154, at *5 (N.J.Super.L.).

Merck aware of this fact, they failed to take any action in response. Given that ACE did not modify the policy language, it is reasonable for Merck to assume that the exclusion applied solely to traditional forms of warfare. Thus, the Superior Court of New Jersey ruled that exclusions in this case only applied to traditional forms of warfare."[11] In 2023, the Superior Court of New Jersey, Appellate Division, determined that not only did the exclusion's plain language support the conclusion, but an analysis of the context and history also led to the same finding. The court affirmed the previous decision.[12] In 2024, Merck and ACE reached a confidential settlement (Pallardy 2024), evading "a New Jersey Supreme Court review of its massive cyberattack insurance dispute on the eve of an oral argument that could have set a national precedent impacting the booming cyber insurance market" (Ebert 2024).

Market response: Lloyd's market association's (LMA) model cyber war exclusion clauses

In response to escalating yet unpredictable cyber risks, London market insurers have revised their model war exclusions to provide clarity and potentially restrict coverage. This effort aims to manage significant exposure and systemic risk. Beginning in 2020, Lloyd's of London mandated that all policies explicitly state whether they cover cyber risks or not.[13] Unless approved by Lloyd's, policies were required to include a suitable clause excluding liability for losses caused by state-backed cyberattacks effective from March 31, 2023. This clause supplements any existing war exclusions and must contain the following minimum provisions[14]:

1. Exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion.
2. (Subject to 3) Exclude losses arising from state-backed cyberattacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.
3. Be clear as to whether cover excludes computer systems that are located outside any state which is affected in the manner outlined in 2(a) & (b) above, by the state-backed cyberattack.
4. Set out a robust basis by which the parties agree on how any state-backed cyberattack will be attributed to one or more states.
5. Ensure all key terms are clearly defined.

[11] *Merck & Co., Inc. v. Ace American Ins. Co.*, 2022 WL 951154, at *5 (N.J.Super.L.).

[12] *Merck & Co., Inc. v. Ace Am. Ins. Co.*, 293 A.3d 535, 551 (N.J. Super. Ct. App. Div. 2023), leave to appeal granted, 298 A.3d 353 (N.J. 2023), and leave to appeal granted, 298 A.3d 364 (N.J. 2023).

[13] https://assets.lloyds.com/assets/y5258-providing-clarity-for-lloyd-s-customers-on-coverage-for-cyber-exposures/1/Y5258%20-%20Providing%20clarity%20for%20Lloyd%E2%80%99s%20customers%20on%20coverage%20for%20cyber%20exposures.pdf.

[14] https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf.

As of January 2023, the LMA also provides two sets of four model clauses, namely LMA5564-LMA5567 A & B (Lloyd's Market Association 2024). Generally, LMA model clauses exhibit similar structures in coverage, particularly regarding events such as war, cyber operations, and cyberwarfare. LMA5564 excludes the aforementioned three factors. In addition to the exclusion for war, LMA5565 excludes "a cyber operation that is carried out as part of a war, or the immediate preparation for a war" and/or "a cyber operation that causes a state to become an impacted state." LMA5566 contains similar exclusions but offers full coverage for other cyber operations. Finally, LMA5567 also includes similar exclusions, but the exclusion pertaining to cyber operations does not apply to "the direct or indirect effect of a cyber operation on a computer system used by the insured or its third-party service providers that is not physically located in an impacted state but is affected by a cyber operation." Furthermore, each A version clause is identical to its B version counterpart, except for attribution. The A version includes attributions of a cyber act to a state, whereas the B version does not (Hill 2023). However, these clauses raise certain concerns, such as the determination of "objectively reasonable inference," attribution, and potential conflicts between different entities. Further observation is needed to understand how insurers will apply such clauses (Al-Shibib et al. 2024).

This brief overview shows that, traditionally, courts tended to include cyber risks in cover, unless they were explicitly excluded in a war exclusion. The market reacted with a more explicit exclusion of cyberattacks in policies. The problem with this approach is that the more risks are excluded, the less attractive insurance becomes. There is, however, yet another disadvantage: (cyber) insurance not only has the advantage of taking on risks from risk-averse individuals through risk spreading; insurers also engage in a form of private governance to control moral hazard risk, thereby also reducing cybersecurity risks.

The rise and fall of private governance and the role of insurance

This paper will further explore how insurance firms and governments collaborate to make up for the mentioned weaknesses in the cyber insurance market. By introducing the insurance as governance theory and examining its application in the realm of cyber insurance, we contend that while a governance effect in managing cyber risk exists, it is limited. However, with government assistance, this function can be enhanced, ultimately benefiting the market.

The rise of insurance as governance

In recent decades, the concept of "insurance as governance" or "regulation by insurance" has gained prevalence and sparked significant debate. This theory posits that insurance serves as a form of private regulation and enhances the function of loss prevention (Scales 2008; Arnold-Dwyer 2023; Mignogna 2018). Proponents apply this theory to a variety of issues, including liability insurance, corporate governance,

cyberattacks, police misconduct, gun violence, environmental pollution, and artificial intelligence (Abraham and Schwarcz 2022; Talesh 2017; Lior 2020, 2022). According to the theory, insurers leverage their expertise to intervene in the conduct of the insured, aiming to improve their quality and governance, and ultimately make such risks more insurable. Additionally, proponents often find that in many cases, the government will intervene in certain areas to support insurance governance. This can include regulating risky activities, investing publicly in risk reduction, and implementing co-insurance schemes (Baker and Shortland 2023b, a).

The limits of insurance as governance

However, critics argue that one should not overstate the potential of insurance as governance. They contend that the actual capacity of insurance to act as a regulatory tool may be limited and that its effectiveness in significantly altering behavior or reducing risks is limited (Abraham and Schwarcz 2022; Talesh 2017). Insurers seldom intervene or are truly able to change the conduct of the insured. The insurance as governance theory likens the governance effect of private insurers to public governance. However, this comparison—particularly in terms of combating moral hazard and enforcing mandatory rules similar to those enforced by governments—is imperfect. Given that experience rating and other loss-prevention mechanisms share similarities with "Pigouvian taxes," which are intended as an alternative to traditional regulation, labeling them as "regulation" seems inappropriate (Abraham and Schwarcz 2022). Essentially, even though social responsibility has become more prevalent in recent decades, insurers primarily "regulate" to reduce their own liability rather than to serve the public interest (Abraham and Schwarcz 2022). The interests of insurers often diverge from the broader interests of society (Logue 2015).

The magnitude of the regulatory effects is also questionable. The capacity of insurers to act as private risk regulators strongly depends on the institutional context and the nature of public regulation (He et al. 2018). This private regulation does not linearly increase with risk exposure. In other words, an increase in risk severity does not result in a proportional increase in insurer regulation (Mendoza 2020). When insureds' risk exposures substantially increase, private regulation by insurers does not escalate correspondingly, as this is contrary to insurers' financial interests (Mendoza 2020, p. 377).

Abraham and Schwarcz (2022) analyzed both conventional and unconventional loss-prevention methods and found that their governance effects are limited. Discussing conventional methods, they explore the impact of risk-based pricing, partial insurance, coverage restrictions, exclusions, and ex post loss management. Although risk-based pricing can identify relevant pricing factors, it rarely pinpoints critical ones that would enhance governance of the insured (Abraham and Schwarcz 2022). In practice, insurers may keep important rating factors confidential, which undermines the possibility of reducing risk. Insureds usually lack sufficient capacity to adjust their behavior to fit risk factors effectively (Abraham and Schwarcz 2022, p. 238–241). Additionally, while the costs of precautions are certain and immediate, the benefits of premium savings are

prospective and uncertain (Abraham and Schwarcz 2022, p. 242–243). These factors all give insureds weak incentives to modify their behavior.

Unconventional loss-prevention methods refer to strategies that go beyond the traditional processes of insurance to mitigate risks (Lior 2022). While insurers sometimes offer guidance, influence, and training to help insureds prevent losses, Abraham and Schwarcz (2022) argue again that such initiatives are not widespread. Additionally, providing specific instructions, as opposed to general advice, can expose insurers to greater liability risks (Abraham and Schwarcz 2022, p. 258). These factors contribute to the limited adoption and effectiveness of unconventional loss-prevention measures in the insurance industry.

Summary

The evolution of the theory of insurance as governance encompasses both positive and negative perspectives, each with limitations. Even supportive research acknowledges that insurers do not monitor the insured without considering their own interests, and it is not assumed that these interests will always align with the public good. Critics of the theory often argue that its optimistic view of the governance function of insurance is overstated, yet they rarely deny its existence outright (Baker and Shortland 2023b, a). This suggests that positive arguments may complement and coexist with the critiques to some extent.

From the analyses above, it appears that there is no complete conflict between the mentioned theories. None of them provides convincing evidence either in support of or against the hypothesis that insurers would engage in private governance related to cyber insurance. The basic problem is that cyber risks are so new that insurers often lack relevant experience and information to adequately assess cyber-related risks and to prescribe efficient preventive measures (Nieuwesteeg 2018). It is therefore not surprising that some have argued that for cybersecurity, risk-sharing contracts between operators may do a better job than insurance, as in some cases operators might have better information to enable an effective mutual monitoring than insurers (Faure and Nieuwesteeg 2018).

Insurance of cyber risks and its governance effects

We now turn to the question of whether and how it is possible to engage in insurance as governance in the field of cyberwar risks and what are the impacts on incentives for *ex ante* cyberwar-risk mitigation. We also discuss one important difficulty: whether cyberattacks can be attributed to a state and can thus be considered a warlike activity.

Insurance of cyber risks

Currently, there is no universal definition of cyber risks. The term “cyber risk insurance” broadly relates to or covers similar terms such as “cybersecurity insurance,”

"cyber liability insurance," and "cyber loss insurance" (Rice 2019; Hunt 2019). Generally, cyber insurance provides coverage for both first-party losses and third-party liabilities (Talesh 2018). Damages covered by first-party cyber insurance include damage to insureds' intangible property, restoration costs, business interruption costs, property losses, and expenses arising from distributed denial of service (DDOS) attacks, theft of property, and cyber-related extortion, and others (Rice 2019). Meanwhile, third-party cyber insurance covers liability risks and defense costs (Rice 2019, p. 21).[15]

Recent literature presents varied opinions regarding the governance effect of cyber insurance. Some papers suggest that cyber insurers have a broad regulatory effect on the market, improving both the conduct of insureds and the overall market environment. This is because "insurers have unique abilities and incentives to inform firms of their legal obligations, develop best practices, audit and educate firms about these practices, and lobby for improvements to the overall state of the cybersecurity ecosystem" (Hurwitz 2017). Cyber insurers can alleviate the impact on victims and enhance the loss-prevention mechanisms of their clients. They may require insureds to implement baseline security practices before issuing policies and provide regular checkups and preventive measures. Additionally, they offer professional assistance for victims after losses have occurred (Westbrook 2022). Thus, insurers provide not only insurance but also risk management services aimed at enhancing insureds' cybersecurity profiles and reducing their risks (Talesh and Cunningham 2021). Insurers have significant power to lobby and promote their products and services, while the opposing side—usually consumers with less power and less cohesion—has a diminished ability to push back (Hurwitz 2017). Consequently, cyber insurers play a regulatory role over their insureds (Talesh and Cunningham 2021). In contrast to D&O (directors and officers), insurers who usually do little in terms of loss prevention and monitoring, cyber insurers are believed to provide substantial risk management services and actively influence insureds' handling of data and cybersecurity, based on the empirical research examining the governance effect of various types of insurance (Talesh 2018). More specifically, ransomware insurance also provides significant support both before and after a cyberattack (Logue and Shniderman 2021).

However, some researchers found insurers' role in governance and loss prevention is limited and subject to certain conditions. For example, Vicevich (2018) argues that while cyber risk is best addressed through insurance, the private insurance market alone is unable to successfully manage cyber risk comprehensively. Baker and Shortland (2023b, a) find that insurers only selectively engage in security and monitoring, rather than consistently applying these practices across all policies. Abraham and Schwarcz (2022) lso argue that insurers can limit risks through underwriting, which may deter them from benefiting from or advocating for standardized security standards. Consequently, cyber insurers have done little to promote public policies or broader security standards across industries. Additionally, their critique of coverage restrictions and exclusions in conventional insurance methods resonates with previous analyses concerning cyber insurance and war exclusions. The insurance

[15] § 200:8. Cyber liability policy and duty to defend, 14 Couch on Ins. § 200:8.

market, including the LMA, has been quick to clearly exclude potential war risks in cyber insurance policies. This response primarily serves to protect insurers from the risk of war but does not encourage insureds to manage war-related losses effectively. Hurwitz (2017) more comprehensively examines the limitations of cyber insurance governance. Although cyber insurance is developing, its depth and breadth still require improvement. Moreover, many of the coverages and exclusions are ambiguous and controversial. Insurers tend to interpret exclusions broadly, which makes cyber insurance less attractive and diminishes its regulatory effect. Cyber risks often cause significant and comprehensive losses that are difficult for insurers to precisely predict and calculate. Additionally, cyber risks are usually complex and intertwined. Many insureds with similar vulnerabilities can be seriously affected by similar risks. This characteristic contradicts the general insurance principle that "risks cannot be correlated—the fact that one party experiences a loss does not suggest that others are more likely to experience the same loss" (Hurwitz 2017, p. 1539). Consequently, insurers are cautious about writing broad policies, which further restricts the regulatory function of cyber insurance.

Cyber risk is a growing concern, and the issues surrounding claims about war or warlike exclusions are evolving. By implementing more specific and comprehensive exclusions, insurers may be able to more effectively avoid war risks. However, this can also generally diminish the utility of insurance as a risk-spreading instrument, and make it more challenging for the industry and consumers to manage cyber and war risks through cyber insurance. Insureds generally lack the capability to effectively manage such risks. Although insureds may recognize that insurers are concerned about war risks and thus wish to exclude them, this awareness does not necessarily translate into improved knowledge or ability to manage such losses. Insurers seldom engage in diligent post-incident loss management or address post-incident moral hazard. Instead, insurers often simply shift the losses back to insureds rather than reducing them (Abraham and Schwarcz 2022). Despite this criticism, in the realm of cyber insurance, insurers may still provide more extensive post-incident services for insureds than other types of insurance, such as data restoration (Abraham and Schwarcz 2022, p. 252; Talesh 2018).

Insurance as governance in shaping international cyber war and security norms

Socio-legal scholars have consistently posited that private governance typically operates on the foundation of social norms (Grisel 2021), and reflects social efficiency since it is flexible, spontaneous, easy to enforce, and inexpensive (Telesetsky 2017). The role of insurance in shaping global norms for cybersecurity and cyber wars is increasingly explored (e.g., see Shackelford and Wargames 2020; Wolff 2024), "[I]nsurers, …, are instead, through their own efforts to define unacceptable state cyber-activity, nudging those government-led multilateral efforts towards norms centered more on financial costs and interconnected losses."

1. Definition of cyberwar and regulating through insurance policy wording.

Cyber insurers face challenges in handling clauses that exclude war, particularly in defining what constitutes "war" and "warlike activities." As discussed above, a comprehensive property insurance policy from Zurich American Insurance Co. excluded the NotPetya cyberattack based on the following policy term of war exclusion: "Exclusion B.2(a): This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:… 2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any: (i) government or sovereign power (de jure or de facto); (ii) military, naval, or air force; or (iii) agent or authority of any party specified in i or ii above."[16] However, the insurer finally settled with the insured, implying that the court weighed in favor of the insured (CSO 2024; Reinsurance News 2024). Studies also highlight the problem of vague definitions of cyber war, leading to gaps in coverage (Cremer et al. 2024). The lack of a universally accepted comprehension of the definitions enshrined in the war exclusion clause leads to varied interpretations and disputes across various jurisdictions (Geneva Association 2020). The discrepancy in international consensus between the precise behavioral parameters or criteria outlined in the war exclusion clause, which differentiate a cyber event as an act of terrorism or use of force or armed conflict, exacerbates this concern (Woods and Weinkle 2020a). For example, there is a clear distinction between the definitions in the international law of armed conflict and international humanitarian law. The law of armed conflict focuses on when a state may lawfully use force against another state, i.e., the right to declare and wage war (jus ad bellum); in contrast, international humanitarian law focuses on the rules regulating the conduct of combatants during war, i.e., justice in time of war (jus in bello) (National Research Council 2009). In international humanitarian law, the threshold for the "use of force" is not the same as that for an armed attack. In the Nicaragua case, the International Court of Justice recognized certain "most serious" acts as armed attacks and other "less serious" acts as use of force.[17] However, not every state agrees with this view. US law, for example, establishes that there is no significant line between the use of force and an armed attack (US Department of Defense 2015; Goodman 2018).

It is quite common to see revisions in insurance policy exclusions following substantial legal disputes over claims that were rejected due to war-related incidents (Wolff 2021a, b). Compared to comprehensive property insurance policies, Zurich's standalone cyber insurance policy template included a "War or Civil Unrest" exclusion for costs incurred by "(1) war, including undeclared or civil war; (2) warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign, or other authority using military personnel or other agents; or (3) insurrection, rebellion, revolution, riot, usurped power, or action taken by governmental authority in hindering or defending

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

[17] Nicaragua judgment: Military and Paramilitary Activities in and against Nicaragua (*Nicar. v. US*), 1986 ICJ 14 (27 June), para. 191.

against any of these."[18] The Zurich policy explicitly stated that the "War or Civil Unrest" exclusion did not apply to cyber terrorism. During an examination of 56 cyber insurance policies, Woods and Weinkle (2020a) proposed that the growing inclination for cyber insurance to explicitly include coverage for cyber terrorism diminished the effectiveness of war exclusions within these policies. However, the vague nature of these definitions left uncertainty regarding the classification of incidents such as the NotPetya attack. Bateman (2020) also proposed updating exclusion clauses to more effectively tackle the issues presented by cyber warfare and cyber incidents initiated by state actors.

The issue of cyber war exclusions shows both the evolution and limitations of insurance mechanisms. Despite varying interpretations of what constitutes a cyber war operation, the analogous criterion of "magnitude and consequences" (Schmitt 2017) could serve as a yardstick for assessing whether a cyber assault triggers the war exclusion clause in cybersecurity insurance. In essence, if the magnitude and consequences of a cyber operation are commensurate with a non-cyber operation involving the use of force or an armed assault, it amounts to hostile action or a wartime event. This stringent benchmark suggests that most cyber operations will not attain the level of use of force, let alone cross the threshold of an armed attack.

2. Private governance of cyber insurance beyond norms.

Worries about the magnitude and impacts of cyberattacks, along with the failure of global platforms and multilateral governance initiatives to establish international cybersecurity standards, have prompted insurance companies to create their own informal norms (Wolff 2024). Insurers are now delineating particular categories of state-backed cyber activities that they will exclude from their standalone cyber insurance policies or other forms of coverage. Although it is premature to predict the exact influence of these insurer-crafted norms on the formulation of global cyber standards by national governments, some governments are already reacting to the exclusions for state-backed assaults by attempting to define government guarantees and advocating for uniformity in policy terms and exclusions throughout the industry (Wolff 2024). For instance, in June 2022, the US government determined "the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response" through a joint assessment (US Treasury 2022).

While these norms are a significant asset, they also represent the principal vulnerability of private systems because of their broad interpretation and inflexibility (Grisel 2021). In practice, insurers struggle to pinpoint efficient countermeasures and security measures, and they also encounter difficulties in applying current war exclusions to exempt themselves from covering cyberattacks initiated by state actors (Wolff 2021a, b). Unlike norms, rule-based order is characterized by its definitive nature. For insurance to fully contribute to governance, it is essential that a legal structure is established to support it. Legal regulations are the base for insurance

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

markets, as the effectiveness of private governance is constrained by rules and fundamentally rooted in law (Vogel 2018).

To resolve widespread coverage disputes, special rules are proposed to address pervasive disagreements: (a) strengthen the governance function to minimize ambiguity and enhance security, (b) adopt a consumer-protection approach, acknowledging the dominant influence insurance firms wield in defining coverage terms, and (c) recognize the critical role of insurance as a societal mechanism for financial protection and compensation (He et al. 2023). In the case of cyber risks, these rules might (1) reconsider insurance contract interpretation rules to avoid insurers' shifting rather than reducing loss, e.g., reasonable policyholder expectations of coverage for cyber-war-related losses; ambiguity in property coverage for cyber-war-related losses; and contractual manipulations and avoidance of the objection to risk-reducing technologies (Avraham and Porat 2021); (2) encompass guidelines that detail the monetary incentives offered by insurance companies to policyholders who implement risk-reduction strategies; and (3) promote the provision of risk management information by insurers to their policyholders, thereby fostering an increased consciousness of risk as a vital precursor to taking steps to mitigate those risks.

State-backed cyberattacks and the issue of attribution

Attribution is a great challenge and is crucial for applying war exclusions in cyber insurance (Eichensehr 2020). Determining that conduct is attributable to the state is, in effect, determining the appropriateness of the subject of responsibility. If insurers choose to assume the task of identifying state-backed cyberattacks to help determine the exclusion of such incidents from coverage, they may challenge established frameworks and methodologies for attributing cyberattacks. These frameworks are heavily grounded in the belief that states occupy a pivotal, if not primary, role in the attribution of such assaults (Egloff and Smeets 2023).

Despite mirroring similar patterns in traditional settings, including the exclusion of conventional warfare in insurance policies, the cyber context poses additional unresolved inquiries, primarily stemming from the formidable task of identifying the state behind a cyber operation given the vast opportunities for anonymity during such activities (for more discussion about state-backed cyberattacks, see Brunner 2022). One pivotal query that arises is how cyber insurance policies align with, and ought to align with, the principles of attribution under international law. According to international law, there is uncertainty about the attribution of cyberattacks. Generally, cyber actions conducted by an organ of a state or by a person or entity authorized by municipal law to exercise elements of governmental authority are attributable to that state, while cyber activities by individuals or private groups are not (Schmitt 2017). However, cyber actions undertaken by non-state actors may still be attributed to the state if the actions are carried out under the instructions, direction, or control of the government, which recognizes and treats these actions as its own.

Some scholars critique the application of international law in attributing cyber operations, challenging the broad use of war exclusions in policies covering

state-sponsored cyberattacks (e.g., Brunner 2022; Wan 2020). In practice, the primary obstacle in applying the attribution principle lies in the collection of evidence. On the one hand, hackers possess vast means to conceal their identities, and verifying classified data pertaining to cyber assaults is challenging. On the other hand, insurers struggle to access classified intelligence gathered by government agencies. Moreover, attribution encounters geopolitical complexities, as nations strive to outdo each other in disseminating attribution information regarding cyberattacks and exaggerate their technological prowess in the face of uncertainty. Furthermore, it is possible that states may wish to help their citizens collect insurance, which could create a third-party moral hazard (for more on third-party moral hazard, see Parchomovsky and Siegelman 2022).

Summary

Cyber insurance plays a significant role in managing and mitigating the risks associated with cyberattacks, but its effectiveness and governance impact are still evolving. Some argue that insurers act as de facto regulators, encouraging insured parties to adopt stronger cybersecurity practices. However, others contend that the governance role of insurers remains limited. In the context of cyber insurance, issues such as war exclusions and attribution challenges persist, requiring further clarification. This aligns with previous findings: while the governance effect of insurance is evident, it has its limitations, underscoring the importance of appropriate solutions, such as government intervention.

Institutional solutions for insuring cyberwarfare and justification for a public–private partnership

Government intervention

Government intervention via a public–private partnership, whereby the government either acts as the reinsurer of last resort or provides an additional layer of coverage, is theoretically debated. Some economists are very critical, arguing that this will lead to an undesirable subsidization of insurance by the government, disturbing the market phenomenon.[19] It is also feared that the government will not set premiums that reflect market prices (see Levmore and Logue 2003). There are, however, also arguments justifying this type of government intervention. The most important one is that, without state intervention, insurance coverage for cybersecurity risks might simply not have developed.[20] Government reinsurance could then be considered as an adequate method to increase insurability (Kunreuther and Michel-Kerjan 2004). Of course, government reinsurance should correspond with particular conditions. The government should charge an actuarially fair premium, should only intervene to

[19] This criticism comes especially from Gron and Sykes (2002, 2003).

[20] It is a point inter alia made by Harrington (2000).

stimulate the functioning of the market, and should withdraw when the market can take over (Bruggeman et al. 2010).

In practice, one cannot, surprisingly, observe many of these types of government interventions in the field of new and evolving risks. Insurers often lack the capacity to fully manage all risks independently, and government-backed programs, such as the Terrorism Risk Insurance Program (TRIP), the Federal Deposit Insurance Corporation (FDIC), or the National Flood Insurance Program (NFIP), are often advocated by researchers for managing insurance areas including cyber risk (US Department of the Treasury 2016; Macauley and Cotter 2023; Vicevich 2018; Rapela 2021; French 2021), gun violence (Kochenburger 2014), weather-related risks (Ben-Shahar and Logue 2016; MacDougald and Kochenburger 2013; He 2016), political risk insurance (Strong 2015), catastrophe risk (Bruggeman et al. 2010; He and Faure 2018), health insurance (Jost 2009), and even financial crises (Faure and Heine 2011).

Most recently, the piracy crisis off the coast of Somalia (2000–2017) was addressed by the public–private cooperation between NATO and Lloyd's, where the role of marine underwriters at the London market was seen as "silent" security professionals (Lobo-Guerrero 2012). Lloyd's has collaborated with NATO to address mutual worries around marine piracy, aiming to proactively reshape the strategic security landscape of their risk mitigation framework. Even though the NATO/Lloyd's alliance as the solution to Somali piracy might be overstated,[21] the relationship elevates the "fundamental" concept of indemnification to a global arena, where safeguarding capital merges "prudent business acumen" with NATO-inspired strategic security. The practice of insuring marine war risks, like piracy, in this regard is not merely governed by the principle of indemnification; rather, it is centered on embracing risk. By examining the security apparatus through the lens of a moral economy, the proactive stance of Lloyd's Joint War Committee (JWC) is uncovered in rendering maritime war hazards insurable, and thus, governable.

Empirical evidence highlights current challenges in cyber insurance and the necessity for government intervention. Although demand for cyber insurance is increasing, premiums have significantly soared due to various factors, including the cost of remediation, the complexity of coverage and underwriting, the lack of historical data, the cost of reinsurance, and coverage limits and exclusions (Entech n.d.). In the US, cyber insurance premiums increased by 28% on average in the first quarter of 2022 compared to the fourth quarter of 2021. With rising premiums and reduced coverage, firms are finding it increasingly difficult to obtain cyber insurance, leading to a contraction in the market (Violino 2022). Direct written premiums for cyber coverage in standalone and packaged policies declined for the first time in 2023 by a modest 2%, a sharp contrast to the market growth of approximately 200% from 2000 to 2022. This reversal occurred despite continued growth in demand for coverage (Fitch Ratings 2024). Renewal rates for cyber insurance also declined for three consecutive quarters, including a 4% drop in the fourth quarter of 2023 (Fitch

[21] Some opinions state that the turning point for Somali piracy was a change in government regulation in 2011, permitting the use of private armed security guards on ships. Naval protection on its own had only very limited effects on deterring and disrupting piracy. See the reviewer's comments on file.

Ratings 2024). This evidence underscores the need for government intervention to address these challenges and stabilize the market (ISA n.d.).

Justification of insurers' actions

One way for insurers to improve insurability is to cooperate via collective actions, for example, exchange of information on cyber risks. However, two specific problems may arise. First, it may be complicated for insurers to cooperate in the area of cybersecurity. However, cooperation between insurers could generate large economies of scale, given the limited knowledge available on the mitigation of cyber risks in the market. Because variation in cyber risks is wide, it may be difficult to organize cooperation among insurers. The problem is not only that the market is very dispersed, but that there is also a high degree of competition. A second issue is that concerns may arise that such actions could constitute collective action and potentially violate antitrust laws, particularly when insurers collaborate to improve insurability. However, such concerns are generally limited. For instance, under US law, collective action requires the following elements: the existence of "a conspiracy or an agreement among two or more persons," an intention or purpose to "restrain or harm competition," and the actual result of restraining or harming competition (Flatt 2009).[22] In the context of the insurance as governance theory, insurance is viewed as "an institutional force that affects individuals, organizations, and institutions both within and outside the insurance industry." The private insurance industry often shares "similar goals of security and solidarity through the pooling of risks, using similar techniques for governing at a distance, and collaborating within insurance regimes" (Ericson et al. 2003). These mechanisms do not necessarily involve the elements of collective action, such as conspiracy, agreement, intention, or any result that restrains or harms competition.

Secondly, due to the unique nature of the insurance business, certain exemptions to antitrust laws typically apply. Under the McCarran-Ferguson Act, the US grants the insurance industry a conditional exemption from federal antitrust laws. This exemption applies only if (1) the activity is related to the business of insurance, (2) the business is regulated by state law, and (3) there is no involvement in practices such as boycotts, intimidation, or coercion (McGuire 1994). The rationale behind this exemption is to allow flexibility in insurance industry practices, such as information sharing (Malone 2021). Therefore, limited or appropriate sharing of information and cooperation between insurers generally falls within these exemptions and does not violate antitrust laws. While collaboration between insurers could potentially harm competition, such cases are expected to be rare, and antitrust intervention remains necessary when competition is at risk.

Also, sometimes the governance influence of private insurers is more indirect and milder, with market participants often being influenced by industry leaders. For

[22] *American Tobacco Co. v. U.S.*, 328 U.S. 781, 810, 66 S. Ct. 1125, 90 L. Ed. 1575 (1946); see also *Monsanto Co. v. Spray-Rite Service Corp.*, 465 U.S. 752, 764, 104 S. Ct. 1464, 79 L. Ed. 2d 775 (1984).

example, Lloyd's holds around 20% of the global cyber insurance market.[23] While this is not yet dominant, its modifications to cyber insurance clauses still attract significant attention within the market. Similarly, Lloyd's is widely considered to have a dominant position in marine insurance, holding approximately 28.2% of the global marine insurance market.[24] Even though Lloyd's does not intentionally collaborate with others in the market, its presence, practices, and customs are substantial enough to shape industry trends (Ragozino 1998).

Institutional solutions for promoting insurers' governance of cyber risks

1. A new conceptual framework.

Building on previous research, many studies have found that while the governance effect of insurance is limited, government involvement remains indispensable and beneficial in supporting private regulation by insurers. Much of the literature on the insurance as governance theory, whether supportive or critical, ultimately concludes or recommends that there should be support from the government or involvement through public–private partnerships. Private regulatory tools, such as insurance, might not only be more effective and cost-efficient than direct government interventions, they may also sidestep the political concerns associated with public regulation (Kochenburger 2014). It is not feasible to rely solely on insurers as regulators. For certain risks, insurers' incentives to minimize losses can effectively supplement government regulation. However, for other risks, government intervention remains the only viable option (Logue 2015). While insurers' outsourcing of regulatory roles works best where government regulation faces challenges (Trang 2017), private regulation should be seen as a valuable adjunct to a system of public regulation rather than a standalone solution (Scales 2017).

In recent years, Baker and Shortland (2023b, a) have developed a new conceptual framework that builds upon and refines the insurance as regulation theory. They use five types of crime as examples—auto theft, art theft, kidnap and hijack for ransom, ransomware, and payment card fraud—to illustrate how insurers collaborate with other entities to control crime across three dimensions. Insurers can firstly stimulate insureds' demand for security measures, then may partner with third parties to shape the incentives, and finally engage with government agencies to help control crime and lobby to modify laws to mandate insurance coverage and control criminal profits (Baker and Shortland 2023b, a). This theory resonates with many previous studies that have underscored the importance of cooperation between the public and private sectors in addressing complex issues like crime and security.

Baker and Shortland (2023b, a) also provide a comprehensive analysis of government intervention in insurance markets from a three-dimensional perspective,

[23] https://www.insurancetimes.co.uk/news/lloyds-receives-approval-for-cyber-syndicate-as-it-targets-pragmatic-growth/1442439.article.

[24] https://iumi.com/news/press-releases/positive-development-across-all-marine-insurance-lines-of-business-continued-in-2023-reports-iumi.

encompassing regulation by risky activity, public investment in risk reduction, and co-insurance. They explore six types of insurance as examples: art theft insurance, terrorism insurance for commercial property, kidnap for ransom insurance, Arctic shipping and marine insurance, environmental liability insurance, and public director and officer liability insurance. Their findings suggest that government plays an active role in the insurance market, extending beyond its traditional regulatory duties. This involvement includes making data collection and relevant information publicly available, which benefits both private insurers and the government itself. Additionally, the government engages in public investment to enhance loss reduction measures, further demonstrating its proactive role in shaping and supporting the insurance landscape.

In the field of cyber risks, they further analyze the development of ransomware-as-a-service (RaaS), and note that growing cyber risks, coupled with higher pricing and stricter underwriting conditions, complicates the cyber insurance market. However, collaboration among insurers, third parties, and the government has helped make cyber risk more insurable. For instance, the Ransomware Taskforce, a public–private partnership designed to combat cybercrime, has emphasized the need for government to take a more active role in addressing cybercrime (Baker and Shortland 2023b, a). In response, entities such as the US government's National Cryptocurrencies Enforcement Unit and LMA have also acted swiftly to address these challenges.

2. Institutional solutions for better public–private partnership.

Just after World War II, Hirschleifer (1953) proposed a system of government-provided war damage insurance. He feared that if such a program was not implemented, the political landscape was likely to necessitate compensation for incurred damages. This type of direct governmental compensation could lead to various perverse effects, referred to as the "charity hazard" (Raschky and Weck-Hannemann 2007). Given the divergent theories on the governance of cyber insurance, a public–private partnership is indeed worthy of consideration.

For cyber and ransomware risks, private-sector involvement is crucial because a lot of infrastructure is privately owned. However, the regulation of cyber activities inevitably requires public authority (Vicevich 2018). Additionally, some literature advocates for the establishment of a National Cybersecurity Safety Board (NCSB), modeled after the National Transportation Safety Board, to investigate cyberattacks and support both public- and private-sector efforts.[25] Baker and Shortland (2023b, a) suggest that government intervention could follow this model, including providing co-insurance for catastrophic events, regulating insureds to enhance cyber risk and data protection standards, and offering public investment to combat cyberattacks. Similarly, Logue and Shniderman (2021)

[25] "[Such a consortium-based, decentralized approach to attribution would likewise have the added benefit of incentivizing robust information sharing, which is vital to the overall cause of cyber peace, and which has come under threat given trends toward cyber sovereignty and data localization]," see Shackelford and Wargames (2020).

propose coordinating insurers with the Office of Foreign Assets Control (OFAC) and the government to jointly tackle cyber risks. In this model, insurers and the OFAC could act as private and social regulators for ransom risks, while the government could assist with a mechanism similar to the Terrorism Risk Insurance Program (TRIP) to provide support (Logue and Shniderman 2021). Thus, regardless of the type of government involvement, there are numerous ways that "the government can begin to both make victims whole again and protect its citizens from the inevitability of a cyberattack" (Rapela 2021).

Moral hazard could also emerge in cyber war damage insurance, especially when there are large government subsidies involved. In Hirschleifer's war damage insurance framework, insured individuals or entities would pay premiums tailored to their specific risk of loss, and in the event of a loss, they would be compensated using the pooled premiums (Hirshleifer 1953). This system would impose higher insurance premiums on buildings situated in large cities, which are often prime targets for attacks, or those lacking adequate fire prevention infrastructure. These higher premiums serve as both an incentive and a warning. Conversely, lower premiums in safer areas would motivate decision-makers to consider locating outside major metropolitan areas, given the reduced insurance costs. In essence, the differential in premiums serves as a guide, allowing stakeholders to assess the inherent risks involved in various designs or locations by comparing premium rates, thereby implicitly estimating the hazards they may encounter (Siegelman 2002).

The result of this analysis is straightforward: government intervention in cyber insurance is important, not only for insurability (by providing additional capacity), but also because governments can use their regulatory instruments to increase cybersecurity. In that respect, governments have an advantage over insurers. That is why government intervention, for example in the domain of terrorism-related risks, has been defended; terrorist attacks are often aimed at governments and so governments may be best placed (given economies of scale) to take measures to prevent them (see, inter alia, Kunreuther and Michel-Kerjan 2005). For natural catastrophes, governments have also successfully intervened as reinsurers of last resort, while also using their regulatory powers to reduce risks. An often-cited success story is the cantonal insurance system setup in Switzerland. Empirical research comparing insurance in Austria, Switzerland, and Bavaria has shown that disaster preparedness is higher and damages are lower in Swiss cantons (see Raschky et al. 2009). This is remarkable as the Swiss insurance system is based on cantonal (state) monopolies (Emons 2001). This model has even been referred to in the literature as "efficient monopolies."[26] The reason behind this success is that the Swiss cantonal governments can on the one hand provide state insurance, but on the other hand use their regulatory powers to impose particular risk-reduction measures. This model could also be effective cyber risks.

3. An effective cyber insurance program in Singapore.

[26] More particularly in the monograph by Von Ungern-Sternberg (2004).

In practice, Singapore is one of the first states to enhance cyber resilience and foster an efficient insurance marketplace. In 2016, the Monetary Authority and Cyber Security Agency, in collaboration with academic experts (Nanyang Technological University) and industry partners, launched the Cyber Risk Management (CyRiM) Project "to tackle demand and supply challenges confronting the cyber insurance marketplace" (Wee 2024). The CyRiM Project encompassed three key elements: establishing a uniform classification system for characterizing cyber security events, constructing a repository of cybersecurity incidents and the financial impacts they entail, and evaluating various frameworks for cyber-related damages to facilitate actuarial costing (Wee 2024). Having observed cyber insurance in the US, the CyRiM Project released a report in 2017, which was skeptical about the capacity of the private sector to progress in the absence of government involvement (Wolff 2022). The lessons Singapore gleaned from the US to bolster the cyber insurance market was that government could initially catalyze growth, yet no US regulations had truly aided insurers beyond pressuring companies into purchasing policies. Consequently, CyRiM formulated its own proposal—a cyber insurance pool sourced from both public and private entities, designed to assist in settling claims and mitigating risks (Heinl 2017).

Since 2018, it has pioneered a government-backed commercial cyber risk pool to create a community for underwriting catastrophic cyberattacks (Evans 2018). According to Singapore's minister for finance, the pool is capable of holding up to USD 1 billion and is financed by a blend of insurance companies and insurance-linked securities, aiming to offer "bespoke cyber coverage" to enterprises across Asia (Keat 2018). Worldwide, Singapore boasts the leading cyber insurance uptake, according to a Sophos survey, with 96% of entities insured and 68% holding standalone policies (Asian Business Review 2024). Almost all entities that secured cyber insurance in the previous year also allocated resources to enhance their cybersecurity measures, and invested significantly in cyber defenses. Projected gross written premiums for the Singapore cyber liability insurance market are anticipated to increase from USD 108.04 million in 2024 to USD 172.82 million by 2029, with a compound annual growth rate of 9.85% over the forecasted years spanning 2024–2029 (Mordor Intelligence 2024).

The issues addressed in Singapore not only show the necessity of government intervention in stabilizing and advancing the cyber insurance market, but also the methods by which this can be achieved. Establishing a viable and long-term public–private partnership for cyber risks should adhere to three key principles. Firstly, governments could partner with insurers to promote the adoption of cyber insurance and guarantee that insurers' market-based operations are respected, encompassing incentives like risk pricing, loss sharing mechanisms (e.g., deductibles, copayment ratios, and coverage caps), and exclusion rules. For example, Singapore's Cyber Security Agency launched the Cybersecurity Certification Scheme to foster good cyber hygiene, aiming to collaborate with insurers to boost the uptake of cyber insurance (IAIS 2023). The Monetary Authority of Singapore (MAS), the financial industry regulator and central bank, also introduced the Cyber Security Regulations and Guidance, which focus on (a) cyber hygiene notices for insurers and agents, covering requirements like securing admin accounts, applying patches, setting security

standards, using network security devices, employing anti-malware, and improving user authentication; (b) technology risk management notices for insurers, requiring identification of critical systems, ensuring system availability and recovery, incident reporting to MAS, and protecting customer data with IT controls; (c) technology risk management guidelines, providing best practices for financial institutions to enhance technology risk governance and IT/cyber resilience (IAIS 2023). Secondly, government intervention should be exercised as a last resort, either as a lender of last resort or provider of reinsurance. This approach ensures that government intervention does not hinder the commercial insurance market, allowing insurers to maintain their leading role in cyber risk management. Additionally, governments' robust credit capacity can span commercial insurance cycles, safeguarding insurers' solvency and reducing their concerns, thereby facilitating the provision of cyber insurance products. In Singapore, direct insurers anticipated that claims related to affirmative and non-affirmative (silent) cyber coverage would be manageable, largely because of existing reinsurance agreements (Goh et al. 2020). Thirdly, domestic actors should work with international partners. The case study of Singapore poses the question: how exactly can a small country create a backstop for global cyber risk? Considering the escalating threat posed by cyberattacks, the Singapore government is investigating a collaborative strategy to address the problem, advocating for a unified global effort to combat cyberattacks.[27] Considering the transnational character of the ransomware menace, Singapore's individual actions within its jurisdiction are insufficient to combat cyberattacks effectively. Therefore, it is crucial for counter-cyberattack efforts to support and participate in a concerted global initiative to tackle the threat.[28]

Concluding remarks

Cyberwarfare is one of the greatest threats to the security of electronic communications and can potentially lead to huge losses. We started by discussing criteria of insurability for cybersecurity and argued that it is not surprising that insurers are somewhat reluctant to cover cyber-related risks. The basic problem is high levels of uncertainty, both related to the probability of an attack, but also the potential damage that may result. Consequently, it is also difficult for insurers to demand risk-reduction measures. As cyber risks are relatively new, insurers may lack the capacity to identify effective measures to increase cybersecurity.

As a result, the availability of cybersecurity cover is minimal and the question arises whether extensive cyberattacks would fall under the war exclusion clause included in many insurance contracts. We showed that the judiciary is generally reluctant to interpret war exclusions broadly, meaning general policies may de facto cover cyber-related risks if they have not been explicitly excluded. And that is what

[27] For more information, refer to Singapore's Counter Ransomware Task Force Report, available at: https://www.csa.gov.sg/docs/default-source/publications/2022/counter-ransomware-task-force-report.pdf?sfvrsn=4fb257bb_1.

[28] Ibid.

insurers increasingly do, for example, in the LMA's model for cyber war exclusion clauses.

We argued that this general exclusion of cyber war can on the one hand be understood from an insurer's perspective, but is on the other hand problematic as it may remove cover to protect exposed parties against risk aversion. But there is another problem with excluding cyber risks from insurance. In the literature, it has been indicated that insurers can and often do play an important role in requiring preventive measures from insureds to reduce moral hazard. Even though this form of private governance could in theory lead insurers to play an important role in reducing cyber-related risks, in practice it is doubtful whether insurers (in the rare cases where cover is available) play that role. Often, there is, in practice, much less risk differentiation than would be predicted by theory. The governance effects of insurance concerning cybersecurity are therefore most likely limited at best.

Given these problems, we argued that there may be an important role for governments. For other catastrophic risks (natural catastrophes, terrorism), where the capacity of the insurance markets is limited, there is an increasing emergence of multilayered systems whereby governments play a role as reinsurers of last resort. We argue that a similar model could play an important role in increasing the insurability of cyber risks. Government intervention could create a double dividend: on the one hand, additional financial capacity could be generated (by providing an additional layer of compensation); on the other hand, governments may be in a better position than insurers to promote cybersecurity by using their regulatory powers to reduce cyber risks. Some jurisdictions (such as Singapore) show that these benefits could indeed be generated if the government were to pursue such a supportive role. This constitutes an example of the three-dimensional model advocated in the literature, whereby the focus is first on promoting cybersecurity by operators through a dual effort from insurers (via private governance) and government (via regulatory powers). Ex post, a multilayered system in which (first) insurers and (next) the government would intervene could equally guarantee substantial compensation to deal with the potentially large losses created by cyber war attacks.

Funding Open access funding provided by National Chengchi University. Chun-Yuan Chen acknowledges the support of the National Science and Technology Council, R.O.C. (113-2914-I-004-015-A1) for this research.

Data availability Not applicable.

References

§ 13:30. Exclusions (general liability)—War-risk exclusions, Practical Tools for Handling Insurance Cases 2: § 13:30.

§ 200:8. Cyber liability policy and duty to defend, 14 Couch on Ins. § 200:8.

Abraham, Kenneth S., and Daniel B. Schwarcz. 2021. Courting disaster: The underappreciated risk of a cyber-insurance catastrophe. *Connecticut Insurance Law Journal* 27: 407–473.

Abraham, Kenneth S., and Daniel B. Schwarcz. 2022. The limits of regulation by insurance. *Indiana Law Journal* 98: 215.

Al-Shibib, Luma S., John M. Leonard, and James A. Goodridge. 2024. Review of cyber coverage developments from 2023—A policyholder's perspective, 2024 WL 877331

Arnold-Dwyer, Franziska, A legal framework for net zero aligned insurance products, *Connecticut Insurance Law Journal* 29: 1, 8 (2023).

Avraham, R., and Porat, Ariel. 2021. Stacking the odds: How insurers make our world riskier. https://law.stanford.edu/eventsarchive/ronen-avraham-buchmann-faculty-of-law-tel-aviv-university-stacking-the-odds-how-insurers-make-our-world-riskier/.

Baker, T. 2008. Embracing risk, sharing responsibility. *Drake Law Review* 56: 561–569.

Baker, Tom, and Anja Shortland. 2023a. How crime shapes insurance and insurance shapes crime. *Journal of Legal Analysis* 15 (183): 195–197.

Baker, Tom, and Anja Shortland. 2023b. Insurance and enterprise: cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance—Issues and Practice* 48: 275, 295.

Baker, Tom, and Anja Shortland. 2023c. The Government behind insurance governance. *Regulation & Governance* 17: 1000, 1013–1014.

Baker, Tom, and Sean J. Griffith. 2009. How the merits matter: directors' and officers' insurance and securities settlements. *University of Pennsylvania Law Review* 157: 755, 827.

Bank of England Prudential Regulation Authority (PRA). 2016. *Consultation Paper | CP39/16: Cyber insurance underwriting risk*. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2016/cp3916 (accessed on Aug. 15, 2024; 31 May 2024).

Bateman, J. 2020. War, terrorism, and catastrophe in cyber insurance: Understanding and reforming exclusions. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_-_Cyber_Insurance_-_Final.pdf. (accessed on Aug. 15, 2024).

Ben-Shahar, Omri, and Kyle D. Logue. 2016. The perverse effects of subsidized weather insurance. *Stanford Law Review* 68:571, 580.

Boom, Van, and Willem,. 2008. Insurance law and economics: An empirical perspective. In *Essays in the law and economics of regulation*, ed. Michael Faure and Frank Stephen, 260–262. Intersentia.

Bortnick, Richard J., and Vincent J. Vitkowsky. 2023–2024. § 14:32. Cyber operations and war exclusions. *Data Sec. & Privacy Law* 2: § 14:32.

Bruggeman, Véronique., Michael Faure, and Karine Fiore. 2010. The government as reinsurer of catastrophic risks? *Geneva Papers on Risk and Insurance* 35: 369–390.

Bruggeman, Véronique., Michael Faure, and Tobias Heldt. 2017. Insurance against catastrophe: government stimulation of insurance markets for catastrophic events. *Washington Journal of Environmental Law & Policy* 7: 380.

Brunner, Isabella, 2022. Insurance policies and the attribution of cyber operations under international law: A commentary, *NYU Journal of International Law and Politics* 55: 179–192, 180

Chen, Chun-Yuan, 2016. D&O insurance, corporate governance and mandatory disclosure: An empirical legal study of Taiwan. *Asian Journal of Law & Economics* 7(1): 19, 57.

Chen, Chun-Yuan. 2017. Functions of directors' and officers' (D&O) liability insurance and litigation risk: An empirical legal study of Taiwan. *NTU Law Review* 12(1):1, 40–41.

Chopra, Angad. 2021. Cyberattack—Intangible damages in a virtual world: property insurance companies declare war on cyber-attack insurance claims. *Ohio State Law Journal* 82: 121, 139.

Cremer, Frank, et al. 2024. On the insurability of cyberwarfare: An investigation into the German cyber insurance market. *Computers & Security* 142: 103886.

CSO. Mondelez and Zurich's NotPetya cyber-attack insurance settlement leaves behind no legal precedent. https://www.csoonline.com/article/574013/mondelez-and-zurich-s-notpetya-cyber-attack-insurance-settlement-leaves-behind-no-legal-precedent.html (accessed on Aug. 15, 2024).

DoD Manual: US department of defense law of war manual, para. 16.3.3.1 (2015).

Ebert, Alex. Merck $1.4 billion cyber hack settlement ends 'Warlike' act claim. https://news.bloomberglaw.com/litigation/merck-1-4-billion-cyberhack-settlement-ends-warlike-act-claim (accessed on Aug. 15, 2024).

Egloff, F., and M. Smeets. 2023. Publicly attributing cyber attacks: A framework. *Journal of Strategic Studies* 46 (3): 502–533.

Eichensehr, Kristen. 2020. The law & politics of cyberattack attribution. *UCLA Law Review* 67: 520–598.

Elliott, Rebecca. 2021. *Underwater, loss, flood insurance, and the moral economy of climate change in the United States*, 210. Columbia University Press.

Emons, Winand. 2001. Imperfect tests and natural insurance monopolies. *Journal of Industrial Economics* 49: 247–268.

Entech. sticker shock: Factors driving cyber Insurance Prices. https://www.entechus.com/blogs/factors-driving-cyber-insurance-prices (accessed on Aug. 15, 2024).

Ericson, Richard V., Doyle, Aaron and Barry, Dean. 2003. *Insurance as Governance*.

Evans, Steve. 2018. Singapore launches first commercial cyber risk pool, *Reinsurance News*, Oct. 29. https://www.reinsurancene.ws/singapore-launches-first-commercial-cyber-risk-pool/ (accessed on Aug. 15, 2024).

Faure, Michael, and Klaus Heine. 2011. Insurance against financial crises? *NYU Journal of Law & Business* 8: 117, 149.

Faure, Michael, and Bernold Nieuwesteeg. 2018. The law and economics of cyber risk pooling. *New York University Journal of Law & Business* 14 (3): 923–963.

Ferland, Justine. 2019. Cyber insurance—What coverage in case of an alleged act of War? Questions raised by the Mondelez v. *Zurich Case, Computer Law & Security Review* 35: 369–376.

Fitch Ratings. 2024. U.S. Cyber insurance maintains strong profits; premium growth slows, https://www.fitchratings.com/research/insurance/us-cyber-insurance-maintains-strong-profits-premium-growth-slows-16-04-2024 (accessed on Aug. 15, 2024).

Flatt, Ethan. 2009. Solidifying the defensive line: The NFL network's current position under antitrust law and how it can be improved. *Vanderbilt Journal of Entertainment and Technology Law* 11: 637, 642.

French, Christopher C. 2021. Five approaches to insuring cyber risks. *Maryland Law Review* 81 (103): 121–127.

Geneva Association. 2020. Cyber war and terrorism: towards a common language to promote insurability. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_war_terrorism_commonlanguage_final.pdf. (accessed on Aug. 15, 2024).

Goh, Joseph, Heedon Kang, Zhi Xing Koh, Jin Way Lim, Cheng Wei Ng, Galen Sher, and Chris Yao. 2020. Cyber risk surveillance: A case study of Singapore. https://www.mas.gov.sg/-/media/mas/resource/publications/staff_papers/mas-staff-paper-no57feb2020-1.pdf (accessed on Nov. 15, 2024).

Goodman, Ryan. 2018. Cyber operations and the U.S. definition of "armed attack". *Just Sec.*, Mar. 8.

Griffith, Sean J. 2006. Uncovering a gatekeeper: Why the sec should mandate disclosure of details concerning directors' and officers' liability insurance policies. *University of Pennsylvania Law Review* 154: 1147.

Grisel, Florian. 2021. *The limits of private governance: Norms and rules in a mediterranean fishery*, 4–14. Hart.

Gron, Anne, and Alan O. Sykes. 2002. A role for government? *Regulation* 25 (4): 44–51.

Gron, Anne, and Alan O. Sykes. 2003. Terrorism and insurance markets: A role for the government as insurer? *Indiana Law Review* 36: 447–463.

Harrington, Scott E. 2000. Rethinking disaster policy. *Regulation* 23 (1): 40–46.

He, Qihao, Michael Faure, and Chengwei Liu. 2023. The possibilities and limits of insurance as governance in insuring pandemics. *The Geneva Papers on Risk and Insurance—Issues and Practice* 48: 641–668.

He, Qihao, and Faure Michael. 2018. Regulation by catastrophe insurance: A comparative study. *Connecticut Insurance Law Journal* 24:189, 236.

He, Qihao. 2016. Mitigation of climate change risks and regulation by insurance: A feasible proposal for China. *Boston College Environmental Affairs Law Review* 43:319, 341.

Heinl, Caitriona. 2017. NTU Cyber Risk Management Project (CyRiM): Roundtable series on optimal governance and regulatory structures to enhance resilience. Roundtable two session report: National market and regulatory structures in Singapore, Sept 28. https://www.ntu.edu.sg/docs/

default-source/academic-services/download-session-report2d9320a8-3677-4117-a76e-e29b63a20826.pdf?sfvrsn=45250cdf_3 (accessed on Aug. 15, 2024).
Herr, Trey. 2021. Cyber insurance and private governance: The enforcement power of markets. *Regulation and Governance* 15 (98): 107–111.
Hill, Andrew. 2023. War exclusions in cyber policies: The important details 3. https://www.wtwco.com/en-au/insights/2023/06/war-exclusions-in-cyber-policies-the-important-details (accessed on Aug. 15, 2024).
Hirshleifer, Jack. 1953. War damage insurance. *The Review of Economics and Statistics* 35: 144 (1953), *Connecticut Insurance Law Journal* 9: 1 (2002).
Holderness, Clifford G. 1990. Liability insurers as corporate monitors. *International Review of Law and Economics* 10: 115, 127.
Hunt, Thomas D. 2019. "The internet of buildings": Insurance of cyber risks for commercial real estate. *Oklahoma Law Review* 71: 397, 451.
Hurwitz, Justin (Gus). 2017. Cyberensuring security. *Connecticut Law Review* 49: 1495, 1537–1538.
International Association of Insurance Supervisors (IAIS), Global Insurance Market Report (GIMAR). https://www.iaisweb.org/uploads/2023/04/GIMAR-2023-special-topic-edition-on-cyber.pdf (accessed on Nov. 15, 2024).
ISA. n.d. Cyber-insurance metrics and impact on cyber-security. https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf (accessed on Aug. 15, 2024).
Jaffe, D., and T. Russell. 1997. Catastrophe insurance, capital markets, and uninsured risks. *Journal of Risk and Insurance* 62: 225.
Jost, Timothy Stoltzfus. 2009. Health insurance exchanges: Legal issues. *Journal of Law, Medicine & Ethics* 37:51, 54.
Keat, Heng Swee. 2018. Speech by minister for finance Heng Swee Keat at the 15th Singapore international reinsurance conference, Oct 29. https://www.mas.gov.sg/news/speeches/2018/speech-at-the-15th-singapore-international-reinsurance-conference (accessed on Aug. 15, 2024).
Knutsen, Erik. 2021. The COVID-19 pandemic and insurance coverage for business interruption in Canada. *Queen's Law Journal* 46 (431): 433–434.
Kochenburger, Peter. 2014. Liability insurance and gun violence. *Connecticut Law Review* 46: 1265, 1296.
Kunreuther, Howard. 2008. Insurability conditions. In *Encyclopedia of quantitative risk analysis and assessment*, ed. Edward Melnick and Brian Everitt, 921. Wiley.
Kunreuther, Howard, and Erwann Michel-Kerjan. 2004. Challenges for terrorism risk insurance in the United States. *Journal of Economic Perspectives* 18: 201–214.
Kunreuther, Howard, and Erwann Michel-Kerjan. 2005. Insurability of (mega-)terrorism risk: Challenges and perspectives. In *Terrorism risk insurance in OECD countries*, 107–148. OECD.
Kunreuther, Howard C., et al. 2013. *Insurance and behavioral economics: Improving decisions in the most misunderstood industry*. Cambridge University Press.
Levmore, Saul, and Kyle D. Logue. 2003. Insuring against terrorism and crime. *Michigan Law Review* 102: 304–311.
Lior, Anat. 2022. Insuring AI: The role of insurance in artificial intelligence regulation. *Harvard Journal of Law & Technology* 35: 517.
Lior, Anat. 2020. AI strict liability vis-à-vis ai monopolization. *Columbia Science and Technology Law Review* 22: 90, 120.
Lloyd's Market Association. Cyber war & cyber operation clauses updated, https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA23-002-PD.aspx (accessed on Aug. 15, 2024).
Lloyd's of London Bulletin Y5258. https://assets.lloyds.com/assets/y5258-providing-clarity-for-lloyd-s-customers-on-coverage-for-cyber-exposures/1/Y5258%20-%20Providing%20clarity%20for%20Lloyd%E2%80%99s%20customers%20on%20coverage%20for%20cyber%20exposures.pdf.
Lloyd's of London Bulletin Y5381. https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf.
Lloyd's. 2015. Business blackout: The insurance implications of a cyber attack on the U.S. power grid 3. Emerging Risk Report. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-lloyds-business-blackout-scenario.pdf (accessed on Aug. 15, 2024)
Lobo-Guerrero, L. 2012. Lloyd's and the moral economy of insurance against piracy. *Journal of Cultural Economy.* 5 (1): 67–83.

Logue, Kyle D. 2015. Encouraging insurers to regulate: The role (if any) for tort law. *UC Irvine Law Review* 5 (1355): 1364–1365.

Logue, Kyle D., and Adam B. Shniderman. 2021. The case for banning (and mandating) ransomware insurance. *Connecticut Insurance Law Journal* 28 (247): 315–316.

Macauley, Anthony J., and Daniel A. Cotter. 2023. Recent developments in insurance regulation. *Tort Trial & Insurance Practice Law Journal* 58: 395, 403.

MacDougald, Joseph, and Peter Kochenburger. 2013 Insurance and climate change. *John Marshall Law Review* 47:719, 730.

Malone, Mason. 2021. Sharing is not always caring: Reevaluating the insurance industry's antitrust exemption and information sharing in the machine-learning era. *Houston Law Review*, 58: 987, 1006.

McGuire, Charles R. 1994. Regulation of the insurance industry after Hartford fire insurance v. California: The Mccarran-Ferguson act and antitrust policies. *Loyola University Chicago Law Journal* 25: 303–356, 312.

Mendoza, Marcos Antonio. 2020. The limits of insurance as governance: Professional liability coverage for civil rights claims against public school districts. *Quinnipiac Law Review* 38:375, 384.

Mignogna, Justin G. 2018. Pokémon Go, augmented reality games, and how the insurance industry will help protect a distracted society from becoming even more distracted. *Rutgers University Law Review* 70: 675, 704.

Mordor Intelligence. 2024. Cyber liability insurance market in Singapore size & share analysis—Growth trends & forecasts (2024–2029). https://www.mordorintelligence.com/industry-reports/singapore-cyber-insurance-market (accessed on Aug. 15, 2024).

Munich Re. 2023. Cyber insurance: Risks and trends 2023, April 28. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2023.html (accessed on Aug. 15, 2024).

National Research Council. 2009. Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities. The National Academies Press, 242.

Nicaragua judgment: Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US), 1986 ICJ 14 (27 June), para. 191.

Nieuwesteeg, Bernold, Louis Visscher, and Bob de Waard. 2018. The law and economics of cyber insurance contracts: a case study. *European Review of Private Law* 26 (3): 371–420.

Otto, René, and Wim Weterings. 2019. D&O insurance and corporate governance: Is D&O insurance indicative of the quality of corporate governance in a company? *Stanford Journal of Law, Business & Finance* 24: 105, 105.

Pallardy, Carrie. Merck's cyberattack settlement: What does it mean for cyber insurance coverage? https://www.informationweek.com/cyber-resilience/merck-s-cyberattack-settlement-what-does-it-mean-for-cyber-insurance-coverage-#close-modal (accessed on Aug. 15, 2024).

Parchomovsky, Gideon, and Peter Siegelman. 2022. Third-Party moral hazard and the problem of insurance externalities. *Journal of Legal Studies* 51: 93, 96.

Patel, Nehal. 2021. Cyber and Tria: Expanding the definition of an "act of terrorism" to include cyber attacks. *Duke Law & Technology Review* 19: 23, 38.

Ragozino, Anthony, Domesticating the United States' Securities Laws: The Ninth Circuit Joins the Majority in Enforcing Forum Selection and Choice of Law Clauses Displacing U.S. Law in Richards v. Lloyd's of London, *Pace International Law Review,* 10: 31, 78 (1998).

Rapela, Sean Andrés. 2021. The ugly truth about cyber insurance & governmental data breaches. *Journal of High Technology Law* 21: 242, 266.

Raschky, Paul, Schwarze, Reimund, Schwindt, Manijeh & Weck-Hannemann, Hannelore. 2009. *Alternative financing and insurance solutions for natural hazards: A comparison of different risk transfer systems in three countries—Germany, Austria and Switzerland—Affected by the August 2005 floods*. alpS GmbH.

Raschky, Paul, and Weck-Hannemann, Hannelore. 2007. Charity hazard – A real hazard to natural disaster insurance? EnvironmentalHazards 7: 321.

Reinsurance News. Zurich settles NotPetya cyber lawsuit. https://www.reinsurancene.ws/zurich-settles-notpetya-cyber-lawsuit/ (accessed on Aug. 15, 2024).

Rice, Willy E. 2019. Cyber-technology torts and insurers' ambiguous obligations to defend professionals and business entities under evolving cyber-insurance contracts: statistical and legal inferences from traditional insurers' declaratory J. *University of San Francisco Intellectual Property and Technology Law Journal* 24: 1, 18.

Scales, Adam F. 2017. Any weapon to hand? An essay on gun regulation and the limits of insurance. *Journal of Tort Law* 10 (23): 37–38.

Scales, Adam F. 2008. The chicken and the egg: Kenneth S. Abraham's "The Liability Century". *Virginia Law Review* 94: 1259, 1265.

Scheuermann, James E. 2018. Cyber risks systemic risks, and cyber insurance. *Penn State Law Review* 122: 613.

Schmitt, Michael N. 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 330–337, 339–347.

Schwarcz, S. 2022. Insuring the 'uninsurable': Catastrophe bonds, pandemics, and risk securitization. *Washington University Law Review* 99: 853.

Shackelford, S.J. 2020. Wargames: analyzing the act of war exclusion in insurance coverage and its implications for cybersecurity policy. *Yale Journal of Law & Technology* 23: 362.

Siegelman, Peter. 2002. A new old look at terrorism insurance: Jack Hirshleifer's war damage insurance after fifty years. *Connecticut Insurance Law Journal* 9 (19): 21–22.

Singapore leads in cyber insurance with 96% adoption rate. *Asian Business Review*, Jun 27. https://asianbusinessreview.com/insurance/in-focus/singapore-leads-in-cyber-insurance-96-adoption-rate (accessed on Aug. 15, 2024).

Singapore's Counter Ransomware Task Force Report. 2022. https://www.csa.gov.sg/docs/default-source/publications/2022/counter-ransomware-task-force-report.pdf?sfvrsn=4fb257bb_1 (accessed on Nov. 15, 2024).

Strong, S.I. 2015. The special nature of international insurance and reinsurance arbitration: A response to Professor Jerry. *Journal of Dispute Resolution* 2015:283, 316.

Talesh, Shauhin A. 2017. Insurance companies as corporate regulators: The good, the bad, and the ugly. *DePaul Law Review* 66 (463): 464–467.

Talesh, Shauhin. 2018. Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law and Social Inquiry* 43: 419.

Talesh, Shauhin A., and Bryan Cunningham. 2021. The technologization of insurance: An empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy. *Utah Law Review 2021:* 967, 973.

Talesh, Shauhin. 2015. A new institutional theory of insurance. *UC Irvine Law Review* 5: 617, 650.

Telesetsky, Anastasia. 2017. The valuable role that private environmental governance might play in managing global fisheries resources. In *Protecting forest and marine biodiversity: the role of law*, ed. Y. Fristikawati, E. Couzens, A. Paterson, and S. Riley, 251–271. Edward Elgar.

Trang, Minhquang N. 2017. Compulsory corporate cyber-liability insurance: Outsourcing data privacy regulation to prevent and mitigate data breaches. *Minnesota Journal of Law, Science & Technology* 18: 389, 409.

US Department of the Treasury. 2016. *Guidance concerning stand-alone cyber liability insurance policies under the terrorism risk insurance program*. Federal Register 81, no. 248, Dec 27. https://www.federalregister.gov/documents/2016/12/27/2016-31244/guidance-concerning-stand-alone-cyber-liability-insurance-policies-under-the-terrorism-risk (accessed on Aug. 15, 2024).

US Department of the Treasury. (2022). Potential federal insurance response to catastrophic cyber incidents. Federal Register. https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents (accessed on Aug. 15, 2024).

Van UngernSternberg, T. 2004. *Efficient monopolies: The limits of competition in the European property insurance market*. Oxford University Press.

Verstein, Andrew. 2022. Changing guards: Improving corporate governance with D&O insurer rotations. *Virginia Law Review* 108: 983, 1007.

Vicevich, David L. 2018. The case for a federal cyber insurance program. *Nebraska Law Review* 97:555, 593.

Violino, Bob. 2022. Rising premiums, more restricted cyber insurance coverage poses big risk for companies. https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html (accessed on Aug. 15, 2024).

Vogel, S.K. 2018. *Marketcraft: How governments make markets work*, 25. Oxford University Press.

Wan, K.S. 2020. NotPetya, not warfare: Rethinking the insurance war exclusion in the context of international cyberattacks. *Washington Law Review* 95: 1595.

Wee, Bernard. A bold approach to cyber risk management. https://www.mas.gov.sg/news/speeches/2016/a-bold-approach-to-cyber-risk-management (accessed on Aug. 15, 2024).

Westbrook, Amy Deen. 2022. A safe harbor for ransomware payments: Protecting stakeholders, hardening targets, and defending national security. *NYU Journal of Law & Business* 18: 391, 460, 469.
Wolff, J. 2021a. Cyberwar By almost any definition: NotPetya, the evolution of insurance War exclusions, and their application to cyberattacks. *Connecticut Insurance Law Journal* 28 (1): 85–129.
Wolff, J. 2024. The role of insurers in shaping international cyber-security norms about cyber-war. *Contemporary Security Policy* 45 (1): 141–170.
Wolff, Josephine. 2021b. *How the NotPetya attack is reshaping cyber insurance*, Brookings, Dec 1. https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/
Wolff, Josephine. 2022. *Cyberinsurance policy: Rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks*, MIT Press.
Woods, D.W., and J. Weinkle. 2020a. Insurance definitions of cyber war. *The Geneva Papers on Risk and Insurance—Issues and Practice* 45: 639–656.

About the authors

Qihao He is a Professor at College of Comparative Law, China University of Political Science and Law. He holds an S.J.D degree from the University of Connecticut Law School in the United States. His research focuses on insurance law and financial regulation.

Michael Faure is a Professor of international and comparative environmental law at Maastricht University and Professor of comparative private law and economics at Erasmus School of Law, both in the Netherlands.

Chun-Yuan Chen is a Professor at National Chengchi University in Taiwan (R.O.C). He holds Ph.D. degrees from the University of Illinois Urbana-Champaign, National Chengchi University, and the China University of Political Science and Law. His research focuses on risk management and insurance law.