If Cyber Is Uninsurable, the United States Has a Major Strategy Problem

Abstract

The latest US national cyber security strategy makes a brief but important mention of the role of insurance in protecting the nation from cyber risks. This has become a salient reliance on an unpredictable actor, given the constraints on capital in the global cyber insurance market. While insurers have become more comfortable with cyber risk, there are still elements of it with which they are uncomfortable, particularly systemic and catastrophic risks. Unless insurers can find a way to get comfortable with systemic risk, there will remain a crack in the economic security elements of national cyber security strategy – in the United States and around the world. In order to meet the strategic expectations of the United States, the cyber market will need to continue its growth trajectory, with fresh sources of capital the key to successfully doing so.

Keywords: Cyber Insurance, Insurance Linked Securities, Economic Security, Catastrophe Bonds, Cyber Reinsurance, Public Sector

1 Introduction

Cyber security strategy in the United States appears to be built on a fundamental contradiction – one that is sufficiently severe to call into question the strength and reliability of existing approaches. While cyber security strategy presupposes the existence of a reliable cyber insurance market, some corners of the market itself have been quite vocal in proclaiming that cyber risk is uninsurable. The uninsurability of cyber risks is certainly not a consensus view across the insurance industry, but the ongoing debate suggests a potentially significant problem for cyber and economic security strategy and policy. The foundational contraction has direct and profound national security implications.

The most recent US national cyber security strategy leans heavily on private sector support, to include the insurance industry. Strategic Objective 3.6 focuses on the development of a federal cyber insurance backstop to 'support the existing cyber insurance market' (Biden 2023 22). This leads to a unique predicament. Although it is unlikely that a cyber event would ever become large enough for such a backstop to become necessary, the presence of one could increase insurance industry confidence in their ability to write cyber insurance profitably (Johansmeyer 2024). This could become useful engaging insurance executives who still doubt the insurability of cyber, which in turn would increase the robustness and reliability of the insurance market, thus making cyber insurance a more reliable economic security lever within the context of national cyber security strategy.

Several of the global insurance industry's leading voices take the view that cyber risk is not insurable, claiming that the potential effects of systemic cyber are too vast. Further, they believe that the threat environment is too dynamic and simply too new to reasonably understand. Should the worst of worst-case cyber attack scenarios occur, according to such thinking, the consequences would be virtually unimaginable. What results is an inherent contradiction in the market – where the government relies on cyber insurance as an economic security lever and the insurance sector is reticent to commit to the risk – that could ultimately undermine the US cyber security strategy. If cyber is not insurable, then there is a significant vulnerability in the economic component of cyber security strategy. Yet, the very real flow of capital demonstrates the insurability of cyber and at least a partial market commitment to the class of

business. The result is uncertainty about the future growth of the cyber insurance market and whether the product could be expected to remain available following a major event.

To understand whether cyber insurance is positioned to provide the economic security that states need in the cyber domain, interviews conducted with eleven cyber insurance executives reveal why they are comfortable with the insurability of cyber risk, the steps they take to manage the more difficult aspects of the risk, and the larger systemic concerns that remain a threat. Further, their views offer insight into how systemic cyber risks could be further mitigated, to the benefit of both the cyber insurance market and society. The use of new sources of capital to help transfer cyber risk outside the traditional insurance and reinsurance ('re/insurance') system could make it even easier for the market to absorb more cyber risk and manage it appropriately. Ultimately, that would not only speak to the insurability of cyber but new ways to grow the class of business significantly, ultimately increasing its value as part of a robust and comprehensive cyber security strategy.

This article makes an original contribution to the literature on cyber security and its relationship with economic security via the re/insurance market by showing not just that the insurance industry largely views cyber risk as insurable, despite some prominent voices to the contrary, but also by linking the market perceptions among cyber insurance industry executives with additional ways to increase the flow of capital to the cyber re/insurance market. By using the capital markets for support in transferring major cyber event risk and then government backstops to increase insurance industry comfort and confidence, it may be possible to fuel further cyber re/insurance market growth, ultimately contributing to both cyber and economic security. US cyber security strategy already relies on the cyber re/insurance market. This paper shows how to make the re/insurance industry an even more effective security partner for the US government and the people it serves.

2 Research Methodology

This article uses a mixed-methods approach to research, including both primary and secondary research. The effort begins with a compilation of key industry metrics to construct a foundation for understanding the nature, composition, and depth of the cyber re/insurance and insurance linked securities (ILS) market. The data comes from a wide range of publicly available data sources and existing publications. The sources provide the information necessary to create a reference point in this article for the remarks of the interview subjects on the insurability of cyber. Many of the sources used are from blog posts, company reports, and other materials that are not peer reviewed and are otherwise generally seen as substandard in academic publishing. Not only is there no suitable alternatives, but the value of contributions by journalists (as an example of those outside academia in general) has been affirmed by Brantly (2020 111). In cyber insurance scholarship, the use of company reports and other non-academic sources for information such as industry size and premium, is exemplified in Cellerini et al. (2022 15), Pain (2023 10), and Braun, Eling, and Jaenicke, whose dated $6.9 billion premium estimate comes from a Swiss Re blog post (2023 684, Bundt 2021). This establishes the necessary context for the qualitative research that follows, which brings new and unique insights from a small group of subjects that represents a large portion of worldwide cyber insurance premium.

The primary research on the insurability of cyber risk in this article comes from semi-structured interviews with eleven cyber insurance executives from the Continental Europe, the United Kingdom, and the United States. The interviews were conducted and recorded using Microsoft Teams and ranged from 30 minutes to 60 minutes, with each participant interviewed once between 24 March 2023 and 14

September 2023. The eleven participants represent 42% of the global cyber insurance market, as measured by premium relative to a total market size of $13 billion in premium (Johansmeyer 2023b). Although the sample size may appear to be quite small at first glance, the highly concentrated nature of the cyber insurance market offers no alternative to qualitative research. Adding only four more companies could take the market share up fifteen percentage points. This is based on the four companies contacted but not participating in this study. Three were willing to participate but needed more time due to scheduling challenges. The fifteenth company did not respond (a very small insurer). The collective market share of companies contacted but not participating is approximately $2 billion, or 15% of the global cyber insurance market by premium. Finally, the engagement level with the market is consistent with the nine selected in an insurance-related qualitative study conducted for this journal by Woods and Simpson (2017 212).

The eleven participants in this study (of fifteen contacted) were chosen because together they not only represent a large portion of the market, but they also bring in diverse perspectives. Three of the five largest cyber insurers in the world are represented among the participants, as well as five with $300-700 million in premium to represent mid-sized players and three with below $300 million to integrate the perspectives of smaller players. Rather than simply gather market share in an attempt to gain credibility through scale, this cohort was assembled specifically to gather perspectives from across the market, with the recognition that more insurers from each category would likely yield redundant information. In fact, redundancy of perspective had already become evident, which is part of the reason why three of the companies contacted but not participating were not pursued further. The eleven participants provide a thorough and balanced view of the market.

3 Literature Review

This article addresses how the insurance industry's debate over the insurability of cyber risk could ultimately create a security strategy problem, because national security strategies and their cyber components increasingly contemplate an important role for the re/insurance industry in economic security via the cyber domain. It is important to note that this is not a problem of coordination or collaboration. The US national cyber security strategy's reference to private market contributions, including that implied regarding cyber insurance, does not come with the consent or partnership of the insurance industry. It effectively treats cyber insurance as a 'found object', and there are no requirements that insurers continue to support cyber insurance products.

The extent to which cyber threats are securitized (i.e., treated as security priorities) – and how such securitization is intertwined with other sectors, particularly economic security – is evident through the development of national security strategies (NSS) and national cyber security strategies, documents that reveal a state's security priorities and how it plans to address them. The inclusion of cyber in the former speaks to the securitization of the threat, as evidenced by the inclusion of other security sectors in NSS documents over the past decades, and the development of an explicit and standalone national cyber security strategy indicates prioritization of the threat within a state's security perspective. However, it would be hasty to assume that states are steeling themselves for the prospect of cyber war – or even that cyber has become a significant priority.

In US NSS documents, for example, security priorities include pandemic, climate, economic disruption, nuclear proliferation, humanitarian crisis events, and violent extremism, with cyber a lesser security concern – but still securitized (Biden 2022 32, cf. Biden 2021 7). Russia's priorities have pivoted

in part to the Arctic (Buchanan 2021), along with the war in which it is currently engaged and how that reshapes its relationship with the west (Galeotti 2021). For Ukraine, fears of an invasion by Russia and the experience of both the 2014 attack and subsequent activity via the cyber domain certainly shaped the state's security strategy, but the impact was perhaps more subdued than one would expect (Przetacznik and Tarpova 2022 3). In fact, the significant effort that seems to have been expended into Ukraine's energy security strategy (compared to its cyber security strategy) reveals the states priorities quite well (Ukraine 2017). Economic security, broadly, remains an important feature of NSS documents, as evidenced in their extensive coverage, for example, across those published by the United States, United Kingdom (HM Government 2021), Russia (e.g., Russian Federation 2021), and Ukraine (Ukraine 2020). Further, economic security is foundational to national cyber security strategies, due to the fact that cyber threats largely materialize as economic security problems. Cyber security thus fits into a broad and interconnected set of strategic security priorities, particularly with regard to economic security.

Insurance has been identified as a useful tool for increasing economic security, particularly through its ability to finance post-event reconstruction – whether that event is a cyber attack, political violence, an industrial accident, or even a natural disaster (Din et al. 2017 1). Within the international relations community, the importance of insurance for economic security has been noted largely as a result of the conflict in Ukraine. Staguhn and Bandura believe that insurance could play an important role in the reconstruction of Ukraine after the ongoing conflict, with the $20 billion insured loss estimate they reference having grown to at least $26 billion since January 2023 (2023, IUMI 2023). The importance and usefulness of cyber insurance is established by its explicit mention in Strategic Objective 3.6 of the US national cyber security strategy (Biden 2023 22-3), which directly addresses the interplay between the insurance industry, federal government, and cyber risk. The effectiveness of insurance as an economic security lever derives from the fact that it represents a predictable, relatively high-velocity form of capital, given that it is negotiated and enacted before an event and would then pay out under pre-defined and pre-agreed conditions (Grant 2012 5). Although the cyber insurance sector is currently quite small, with only $13 billion in cyber insurance premium driving approximately $400 billion in notional protection (Johansmeyer 2023b). However, this was not always expected.

Woods and Simpson implied back in 2017 that the insurance industry was not prepared to provide the necessary economic security to society with the belief that, '[g]overnment intervention in the cyber insurance market is justified by previous failure of cyber insurance to deliver upon expectations,' adding that it took until around their article's publication to achieve the $2.5 billion in cyber insurance premium industry-wide that had been expected to be achieved by 2005 (2017 211). The sentiment arose again in 2022, that the nonregulatory benefits and incentives associated with insurance are seen positively, 'but insurance has not yet delivered' (Lostri et al. 2022).

Unmet expectations in this regard have become typical of industry pronouncements and results. In 2017, Camillo forecasted '$20 billion or more' in worldwide insurance premium by 2025, but with 2023's $13 billion and no indications of a major change in industry growth rates, this is clearly unrealistic (Camillo 2017 59, Johansmeyer 2023b, Brew 2024). The fact that large customers stopped or reduced their cyber purchasing in 2023 due to price reinforces the conclusion not only that forecasts of rapid growth in 2017 were unsustainable but also that similarly ambitious forecasts today – e.g., Gallagher Re's $80 billion – should be eyed at least with skepticism (Newman et al. 2022 12).

This very conversation represents progress, given that cyber risk was not always viewed as insurable, with caveats used event today, as evidenced by the concern, 'Some of today's cyber risks do not fully meet the typical characteristics of insurability' (Cellerini et al. 2022 2). For re/insurance to be made available in support of any major loss event, it has to be able to be underwritten profitably, and that includes managing systemic and other catastrophic risks. Systemic events represent the primary concern re/insurers have about the risk itself, as evidenced by the ongoing debate over the war exclusion in cyber insurance policies. Joint efforts by Munich Re, the Lloyd's Market Association, and other market participants have led to heavy investments in cyber war exclusion language, ostensibly to protect the balance sheets of re/insurers across the industry (e.g., Golling 2023, Mukhopadhyay 2023). That said, there is little evidence to suggest that the risk warrants the effort. Yet, little in the way of risk analysis, discussion of the threat environment, or even consultation with the historical international relations literature appears to have informed these views. There has been no published attempt at quantifying the risk of cyber war, and the few attempts to quantify systemic cyber in general (discussed later in this section) have significant flaws.

Absent rigorous analysis, one often finds that anecdotes, isolated events, and hypotheticals are used without analytical or theoretical justification. There are several such cases regularly cited as support for the need for a war exclusion, which will be reviewed momentarily, and they are all flawed. To this end, one need only consider Rid's famous claim that cyber war will not and cannot happen, Gartzke's views on it only being possible if a foreign power 'has decided it can stand toe-to-toe with conventional US military power,' and Brooking's and Lonergan's belief that the page has been turned on 'Cyber Pearl Harbor' (Rid 2011 10, Gartzke 2013 68, Brooking and Lonergan 2023). The notion that '[i]t is easier to imagine a catastrophe than to produce it' applies especially to the prospect of war within the broader set of (largely hypothetical) potential cyber catastrophe events (Lewis 2020). To understand how these factors shape the discussion of cyber war, there is no better place to review this problem than NotPetya.

Costing the global insurance industry an estimated $3 billion, NotPetya and its implications for the insurance industry are largely misunderstood (Evans 2018, Johansmeyer 2024b). It is the largest cyber catastrophe event to affect the insurance industry, given that WannaCry's estimated insured loss was only $50-60 million (Johansmeyer 2024c, Evans 2020). However, its impact on the cyber insurance sector was quite small, amounting to only 10% of the $3 billion, with the rest going to the property insurance market. Mondelez and Merck are part of that 90%, according to the PCS bulletin for NotPetya, calling into question whether any war exclusion for cyber insurance would have made a difference.

Whether NotPetya was an act of cyber war, separate from the insurance discussion, begins with the question of whether cyber war is even possible, hearkening back to Rid's thoughts presented earlier in this section. In assessing the potential for cyber war, Rid draws from the Clausewitzian tradition in asserting that war is violent (2012 7-8), and indeed, NotPetya was not. It also helps to recall Gartzke's contention that an act of cyber war, if possible, would require that the aggressor be prepared for a response with commensurate effect, not merely a cyber response. Following NotPetya, no such response occurred. If it were an act of war, it would have instigated an act of war in reply.

One of the challenges associated with the debate over systemic cyber risk – including war – is that both sides use the same cases as proof, merely interpreting them differently. There is no better example of this than the 'blackout' scenario, with both actual and hypothetical examples having entered the debate. The concept is pretty simple. A hostile actor, presumably a state or state affiliate, attacks a

power grid via the cyber domain and takes out power. Chaos ensues. Hollywood loves this example (Castriotta and Hansen 2024), and so does Lloyd's of London, which published a scenario in which a cyber attack causes a power outage in the United States that affects 93 million people for a period of time stretching to 24 hours from some to weeks in total (Lloyd's 2015 4). The economic losses from such an event, as modeled at the time, could stretch from $243 billion to more than $1 trillion. It is a scenario that Camillo calls '[o]f particular concern' (2017 56). Where the hypothetical falls short, though, is that there is ample precedent with regard to power outages with which to gauge how realistic the Lloyd's scenario is.

The 2015 blackout in Ukraine cost only 230,000 people in Ukraine access to power for only one to six hours in 2015 (Przetacznik and Tarpova 2022 3). That is not remotely reflective of the scale or violence needed, per the Clausewitzian tradition, for war. In fact, the effect pales in comparison to blackouts that occur due to natural disasters and other causes. Hurricane Ida left 'millions' without power just in the state of Louisiana without power, with more than 300,000 still without remedy more than a week later (Beard et al. 2021, Waldrop 2021). The most impactful of all blackouts, which affected the northeastern United States and Canda in 2003, left 50 million people for around 29 hours (Eyewitness News 2023). Cyber attacks have not had nearly that destructive power, despite many attempts to wreak havoc.

Finally, such events as the 2015 attack on the Ukrainian power grid really have not become more common. Attempts have, but the quality of those attempts is so low that one has to contemplate the true nature of the threat. According to records in the Cyber Operations Tracker managed by the Council on Foreign Relations, no cyber attacks on energy infrastructure have succeeded in really landing a punch (CFR 2023). Further, although attacks rose with the ransomware epidemic, the first database of catastrophic cyber events and economic losses reveals no such event with at least $800 million in economic loss (adjusted for inflation) since 2017 (ASTIN 2023). The threshold is low enough to ensure the inclusion of even minor events. Not just war but systemic events more broadly – at least with meaningful economic impact – plunged after 2017, despite the 'proliferation of technology … multiplying the potential attack surface for malicious actors' (Camillo 2017 56).

Coming back to insurance, the industry clings to its fear of cyber war despite conceding that the number of losses the industry has sustained from cyber war is 'likely none' (ASTIN 2023). Fear of cyber war, systemic risk, and the unknown in general has kept capital out of the re/insurance market, ultimately limiting the amount of protection it can offer, which actually increases the economic security vulnerability associated with cyber risks (Johansmeyer 2023). Meanwhile, the future of the cyber re/insurance industry and its ability to provide the economic security capabilities that society needs – and governments expect – is difficult to discern. While concerns of systemic events, as discussed above, imply a constraint on the flow of capital into the market, hyperbolic growth projections abound. Taken at face value, they could result in a security vulnerability of their own, a false sense of security due to projections that the cyber re/insurance market is unlikely to achieve.

4 Analysis of Market Data

The cyber insurance market may still be small and new, but it experienced a period of rapid growth. From an estimated $5.5 billion in worldwide premium in 2020, the market grew to $8 billion in 2021 and today stands at $13 billion in 2023 (Johansmeyer 2023b). Insurers cede 50-55% of the risks they assume to reinsurance, which signifies the importance of the insurer/reinsurer relationship

(Cellerini et al. 2022 16). The estimated size of the global re/insurance market as measured by the amount of insurance outstanding ranges from just under $400 billion to just over $500 billion, with the lower end more generally accepted (Johansmeyer 2023b).

The cyber re/insurance market has weathered difficult conditions and found the wherewithal to grow. Issues such as ransomware, which caused unexpectedly high losses from 2019 to 2020 (Baker and Shortland 2022 14, Stark 2021), do suggest that attritional (i.e., day-to-day) losses can become more burdensome than anticipated, but they are hardly catastrophic. During that period, the cyber insurance market's overall loss ratio reached only 67% in 2020 and 67% again in 2021 before coming back down to 2019 levels of 45% in 2022 (Kerman and Clouse 2023 9-10). The 67% loss ratio for 2021 (for the United States but applied worldwide as the best available data) would translate to aggregate annual cyber insured losses for the entire industry of $4.4 billion based on estimated annual worldwide premium of $6.5 billion (NAIC 2022). Despite the high loss ratio, which suggests a sector that is teetering on the edge of break-even after expenses, the aggregate worldwide losses are quite small. Further, they would be less impactful today, given that the cyber re/insurance market's high rate of growth in premium since the difficult ransomware years has come largely without underlying growth to overall cyber insurance limit outstanding (Johansmeyer 2023b).

Despite the fact that premium growth has come largely through a more expensive insurance product, further industry growth is expected to grow quickly in the near future, and it would would have to come through increased market penetration, which suggests some softening of pricing given that rate increases since the ransomware epidemic drove many protection buyers out of the market (Holmes 2022). Reinsurance intermediary Gallagher Re believes that cyber reinsurance premium will reach $80 billion by 2033 (from $6.5 billion in 2023), edging ahead of the size of the property-catastrophe reinsurance market, despite 2023 property-catastrophe reinsurance premium of above $50 billion (Newman et al. 2022 12). The projection requires that the property-catastrophe sector nearly double while cyber reinsurance would spike by a factor of greater than ten. Meanwhile, the growth of the cyber reinsurance market would come without any meaningful change to reinsurance cession rates (around 50%), requiring further capital allocation to cyber risks by reinsurers. The report is silent on where that capital would come from.

If that cession rate holds true, then cyber insurance premium would likely have to reach $160 billion in 2033, with the amount of protection outstanding surging to nearly $5 trillion. If, as discussed above, a softening of prices were to coincide with this projected growth, the amount of protection outstanding could far exceed $5 trillion. No substantiating analysis has been provided to support this forecast. Howden has more modest (but still high) forecasts for more than $50 billion in cyber insurance premium worldwide by 2030, also with little in the way of underlying analysis and considerably optimistic outcomes.

Several forms of reinsurance could help fuel longer-term cyber re/insurance market growth, but new sources of capital will have to form part of the solution. In this regard, the capital markets could help. Long seen as a potential source of capital for cyber re/insurance (e.g., Artemis 2016), ILS market has increased its participation in cyber risks, recently. From a mere $500 million over the five years ending in 2001(Johansmeyer and Mican 2022 53), ILS positions in cyber re/insurance pushed past $1 billion in 2023 (Johansmeyer in Pain 2023 40-1). The issuance of new catastrophe bonds has increased the overall total, although it has been offset by some market exits. Following the three iterations of

insurance company Beazley's private cyber catastrophe bond in 2023, the company launched a public cyber catastrophe bond issuance in the fourth quarter with a target of $140 million, with additional cyber catastrophe bonds completed by Chubb, AXIS, and Swiss Re (Artemis 2024b).

The four new cyber catastrophe bonds completed in late 2023 amounted to nearly $500 million in new cyber protection, all of it on an event basis rather than in quota share form. Further issuance activity in 2024 brings the total to approximately $800 million (Artemis 2024b). With protection for extreme events specifically rather than broad quota share coverage, in which the reinsurer shares more broadly in the insurer's book, the ILS market developments show some progress, even if it is tentative. The small amount of recent issuance activity provides an alternative form of risk transfer that can growth with time – and it will take time to diversify the market away from quota shares, which represent approximately 90% of all cyber reinsurance since at least 2016 (Parsoire and Heon 2016 22, Lau et al. 2020 17). The process will be slow, though, largely because the small (but growing) use of catastrophe bonds would have to change risk-transfer behaviors among both insurers and reinsurers while simultaneously marshalling capital from outside the global re/insurance system – i.e., from capital markets investors who would have to be convinced of the merits of cyber re/insurance opportunities.

The effects of ILS and other new forms of capital will be slow initially and likely take years to ramp up. As the market matures, the issue of economic security and the role of re/insurance in national cyber security strategy remains a concern. Even with insurability largely addressed, the issue of likability remains. Should the need for cyber re/insurance be exercised by a national security event sooner than the maturation process, an economic security measure anticipated by national security strategy would not be present. Protection for systemic and extreme events remains the key outstanding problem for the cyber re/insurance industry, and as the interview findings below reveal, the matter is not yet settled.

5 Voices of the Cyber Insurance Industry

The activities of the cyber re/insurance industry happen separately and distinctly from the national security strategy apparatus that relies on it. Although there is truth to the insurance industry's commitment to 'social good' (Olson 2016), which would be relevant to the role of cyber re/insurance with regard to cyber security strategy at the state level, re/insurers are first focused on their obligations to their owners. As a result, the cyber re/insurance industry has to be treated as a found object by the security strategy and policy community. Although it is possible for the government to influence the market through such measures as regulation and public/private partnerships, market forces are the ultimate driver of re/insurance company decision-making, which means that states would need to rely on companies that are not obligated to provide security support, coordinate any strategy efforts, or otherwise integrate into cyber security strategic planning on little more than an incidental basis. For this reason, the eleven cyber insurance executives who were interviewed were not asked questions about international relations, cyber and economic security policy, or other overall implications of this research. Instead, the discussions centered on the re/insurance market and its ability to cover cyber risks.

The fact that the eleven cyber insurance executives participating in this study speak to the insurability of cyber risks should come as no surprise. After all, they were selected because they are cyber insurance executives. Although one could choose cynicism and dismiss their views simply because advancing the insurability of cyber risks is in their interests, doing so overlooks a much greater self-interest on the part of insurance companies. If insurers did not believe that cyber is insurable, would they have allowed the executives interviewed for this study to engage in cyber insurance? Would they

have allowed these executives to write as much as they have? If anything, given the historical skepticism shown earlier in this article, the rapid growth of the sector speaks to a shift in how insurers perceive the insurability of cyber risks. Thus, given their engagement and the recent growth of the market, the insurability of cyber is easily established.

It comes as no surprise, therefore, that all respondents indicate that cyber risk is indeed insurable, with some caveats of course, largely because it is so predictable. In fact, they believe that cyber risk is knowable and manageable because loss activity has become predictable. One US-based executive explains, 'We have to be able to have a certain predictability associated with the risk,' which enables insurers to 'quantify and price for it,' confirming that these characteristics are present in the market. A UK-based respondent adds that cyber activity 'happens with a reasonable level of frequency and manageable severity' which inherently supports predictability. Respondents generally feel that they have a good handle on their attritional losses and worry more about systemic and catastrophic losses. This demonstrates a considerable step forward from Knake's view that 'no company has sufficient information to price risk for destructive attacks' (2016), not to mention ongoing concerns about the quantification of cyber risk (e.g., Eling and Schnell 2016 478, IAIS 2020 18).

To keep from being overrun by such potential cyber catastrophe losses, the eleven insurance executives interviewed engage in a wide range of risk management activities. Respondents overwhelmingly indicate that they keep an eye on how much cyber insurance they write, seek diversification within their cyber portfolios, and use cyber as a diversifier in their overall businesses. Several respondents specifically indicated that they not only believe that cyber portfolios can be diversified, but that they actively do so, with one explaining that diversification can be achieved by 'splitting your portfolio across regions across industry sectors and across company sizes, which is what we do.' As to the ability to use cyber as a diversifier, one executive from a large cyber insurer notes, 'The non-correlated exposure from cyber probably helped us diversify away from property.'

Additionally, the interview participants exclude certain problematic risks, or risks they otherwise would prefer not to cover, such as critical infrastructure. While this may seem as though it results in partial coverage for the insured – which it does – the use of exclusions nonetheless makes insurance available for other elements of this risk, ultimately allowing nuance to expand the amount of insurance available rather than relegating the insured to an all-or-nothing situation. The use of exclusions is not unusual in other forms of insurance, and it represents an everyday practice. In the property insurance market, for example, risks such as flood and moving earth are generally excluded (ICRMA 2023, I.I.I. 2023), a sentiment that was amplified by a cyber insurance executive in the United States during the interview process.

Of course, within the discussion of exclusions for systemic cyber events, war came up. In general, insurers tend to have exclusions for war, although there is considerable disagreement among them as to how robust those exclusions may be. Five respondents had very firm concerns about cyber war. An executive, based in Continental Europe, describes cyber war as an 'urgent' systemic risk, spent considerable time on the need for a robust exclusion for it, emphasizing how war losses could be devastating to the insurance industry in the near term and its appetite for cyber risk over the long term. An executive in the United States adds, 'The scenario that scares me the most is probably like, let's say, a few years down the line or whatever it happens if China decides to invade Taiwan and the US gives a fairly robust defense.' However, he adds, 'I think there are definitely systemic possibilities beyond war. I

don't think I'm particularly worried about any of them as far as the very insurability of cyber.' Systemic risk exists and must be addressed, but it hardly equates to uninsurability.

On the other hand, just over half of respondents are either not concerned with war risk or think that further focus on the issue is not necessary. An insurance executive based in the United States indicated that excluding war, infrastructure, and other key systemic problems impacts the commercial viability of the product. Another in the United States explains, 'I don't think of it [cyber war] as any different than crimeware actors, and I think the key thing here from my perspective is it doesn't really matter who hits 'Enter' on the keyboard.' Ultimately, whether it is crime or war, he concludes that the actors are 'just taking advantage of the exact same patches or lack of hygiene.' He sees other systemic problems as more relevant, such as vendor risk management. Another says, 'We cover state actors every day,' continuing that 'there's hype around the importance of the exclusion on an individual risk.' Finally, an executive in the United Kingdom finds a place in the middle; he believes that cyber war could be insured, but it would require a price that customers would not be inclined to pay.

The discussion of exclusions has direct implications for national cyber security strategy. Some of the risks that cyber re/insurers seek to exclude because of their large or systemic nature are exactly the sorts of risk that one would expect them to cover from the perspective of national security. After all, an influx of capital after an attack provides the means necessary for recovery, a point evident throughout the conflict in Ukraine discussed by the Center for Strategic and International Studies (CSIS) earlier in this article. If the insurance industry believes the scale of those attacks would be too big to absorb, though, they either would have to exclude or transfer the risk. Doing so, of course, could come at the expense of states who expect cyber insurance to be available as a matter of national security strategy. Of course, there is value in covering attritional losses, as it helps businesses return to normal faster and more easily. Nonetheless, the thin and scattered coverage available for systemic and catastrophic risks results in a strategic economic security gap.

The solution to this problem could very well be more capital. If insurers had more reliable access to reinsurance, not to mention more variety in structures, it might be possible to assume more seemingly correlated risk. This is particularly true if there were capital providers available comfortable with the volatility of systemic risk (from cloud outage to war) and would provide protection simply for the volatility, a practice that has been in place in the property-catastrophe reinsurance market for decades. New forms of risk transfer and sources of capital as a potential solution stems directly from the problems expressed by the insurers interviewed. Eight of the eleven responding insurance executives raised the concern that a major event could exhaust their reinsurance coverage and then cause the insurer further losses, although some conveyed this sentiment implicitly.

For the eight executives concerned about the magnitude of systemic cyber risks relative to the reinsurance protection they have purchased, the need for further risk transfer is evident. Developing a market for these large but more remote risks would not only help insurers hedge above the caps on their quota share reinsurance, but it would also enable reinsurers to raise those caps, because they would be able to cede out some of the increased systemic risk that raising quota share caps would entail.

6 From Insurance Capital to Cyber Security

Insurers need access to more capital for cyber risks, particularly for the systemic challenges described above. This would allow the market to provide more protection, which would support

society's economic security – ultimately aligning cyber re/insurance market activity (to include profit motive) with the security strategy needs of the states in which they operate. Moreover, there is some merit to this view. A more robust cyber re/insurance market is of course more capable of supporting its target market, society, and state economic security. However, there is a subtler and more important concern: Reliability.

Even if the systemic risks feared fail to materialize, simply being exposed to them requires that insurers keep a certain amount of capital on hand, and without more, they will not be able to extend further protection. New capital could come from several different sources. First, it could come from the existing re/insurance market, although there are limits. Capital could also come from new sources outside the reinsurance system in the form of state support, as evidenced in the early progress made through cyber catastrophe bonds and the ILS market in general. There is no single source of risk capital that will support the continued insurability of cyber risk, let alone further market growth. Rather, each of the sources just noted will likely play a role in both the growth of the cyber insurance market and its attendant benefits for state economic security.

The security strategy community needs to be able to rely on the presence of a cyber re/insurance market that is large, robust, and responsive with regard to strategic expectations. To use a blunt example, if the state forms economic security plans for the cyber domain with the expectation that insurers will have $400 billion in protection outstanding, and that level falls to $250 billion, then an economic security vulnerability emerges. In the past, public statements and private market dynamics may have suggested that a pivot away from offering cyber insurance would form the greatest source of such unpredictability, but the comfort with attritional losses expressed by the cyber insurance executives – and the review of historical data – suggests that the re/insurance industry has indeed embraced the cyber class of business. Instead, what remains is a more difficult question regarding whether the cyber insurance industry can scale in accordance with state expectations for economic security strategy.

Transferring risk to capital sources outside the traditional re/insurance system can help address the problem of systemic risk – in cyber and other domains and classes of business. The ILS market has long been seen as a way to do accomplish that, and it has been used to significant effect for property-catastrophe insurance risks (mostly from natural disaster events) for more than twenty-five years. It is comprised of specialist investment managers who allocate capital to insurance risks, and it has grown by helping re/insurers cede difficult systemic risks to a pool of capital outside the re/insurance system. Today, the overwhelming majority of the sector's $112.3 billion is currently allocated to property-catastrophe risks, but the sector has begun to participate in other risks (Artemis 2024).

The prospect of using the ILS market to support cyber risk transfer out of the traditional re/insurance system has been discussed since at least 2015 (Artemis 2015). Cyber ILS transactions have been transacted by at least seven ILS fund managers as of early 2022, with at least another three coming into the market in the year since and possibly even more given the four new cyber catastrophe bond transactions (Johansmeyer and Mican 2022 53, Johansmeyer 2023b). Several of the cyber insurance executives interviewed, in fact, have used support from the ILS market. The potential role of ILS in the cyber insurance market is still evolving, but its still-fragile potential is clearer than it was even a year and a half ago (Carter et al. 2022 7).

Of course, there are barriers to the further growth of the ILS market, as covered extensively by Johansmeyer and Mican, and the discussion does not need to be repeated here. However, it is clear that there is a good start in place – and that further progress can be expected, a sentiment certainly expressed by all eleven of the cyber insurance executives interviewed. In fact, [six] of them have either used ILS capital or have begun very serious inquiries into doing so – inquiries of the sort that are likely to lead to engagement. One more has had preliminary discussions but sees the value in the ILS market for cyber risk transfer and believes that deeper partnering is only a matter of time.

The need for additional capital – particularly from broader financial markets – to help the cyber insurance industry grow and achieve cyber and economic security largely focuses on major, remote, and systemic events, as has been evident from the discussion of both systemic risk in the prior section and hedging such events in this section. While the depth of the capital markets, with an estimated $250 trillion in global investable capital (Chung 2021), would contribute considerable stability, there is a concern that events of such magnitude that they could not even be absorbed by the capital markets are possible.

The catastrophe bond market is taking on the task of assuming systemic cyber risk, which is largely similar to its role in the property-catastrophe reinsurance sector. However, it is not big enough to make a meaningful dent in demand, and it will struggle to do so, given the reluctance of the reinsurance industry to refocus on covers for systemic risk. Several respondents indicated that reinsurers should provide more support for systemic events specifically. Meanwhile, the rate at which quota shares are used suggests that substantial change is unlikely to come anytime soon, a problem amplified by the discomfort associated with the very systemic risks on which reinsurers would need to focus on this market evolution, which unsurprisingly are linked to the sorts of scenarios relevant to national cyber security strategies.

The cyber catastrophe bonds completed in the fourth quarter of 2023 might provide cause for some optimism, and indeed, a collection of transactions for different specific underlying risk transfer purposes suggests a step forward in scale and flexibility. The transactions were all volatility-focused, indicating an alternative to the traditional reliance on quota shares. At an estimated $50 million in premium spend, though, it still pales in comparison to global cyber reinsurance premium of more than $6 billion (Johansmeyer 2023b). The first step is an important one, but more activity is necessary to move the industry from having proved the concept to having made a strategic commitment.

An influx of new forms of risk transfer and new sources of capital, if the trend continues, could buttress global security strategy planning. The importance of insurance as an economic security tool, established earlier in this article, benefits from increased reliability and resilience. Of course, it also benefits from being able to expand to provide more protection. Increased capital flows to cyber re/insurance provide support for both resilience and growth.

Using cyber security measures to prevent attacks is obviously important, and the ability to recover from such an attack is equally important. Remediation is fueled by capital, and insurance represents a mechanism for injecting capital at a time of economic loss based on certain pre-agreed conditions for payment. Cyber insurance brings predictability to the flow of relief capital after a cyber attack, given that it can be expected to appear if the terms of the relevant insurance policy are met. Further, the rapid flow of capital after an attack can support the acceleration of return-to-normal activities, mitigating the impact of a cyber attack and thus strengthening not just the target, but also the

community it serves. The economic security afforded by a robust cyber insurance market is affected at every link in the capital chain – from insurance to reinsurance to retrocession to prospective government backstops. The original insurance policy that provides relatively high-velocity, predictable capital after a cyber attack requires support from reinsurance capital, which is in turn bolstered by the retrocession market and any government mechanisms that would provide theoretical capacity and real comfort.

7 Conclusion

The United States has indicated a strategic reliance on the global cyber re/insurance industry, with the mention in the US national cyber security strategy carrying implications far more profound than its brevity may imply. Cyber security is an economic security problem – at least as much as it is a military, political, or societal problem. The speed and effectiveness of recovery from a cyber attack often comes down to the availability of capital to use in such activities. Insurance, of course, could play a role in minimizing the impact of cyber attacks by accelerating a return to normal. However, the role that insurance could play in US cyber and economic security is a voluntary one. If the insurance industry chooses not to participate, the United States loses that economic security lever.

The notion that cyber is not insurable stands to threaten the market's access to cyber insurance protection, which would in turn leave a gap in the US national cyber security strategy. Insurance does little good if it is not available. As a result, the debate in the insurance industry over whether cyber is insurable represents a significant concern to the nation's strategic security. While there are some prominent voices expressing skepticism as to the insurability of cyber, the market itself appears to have voted with its capital. Insurers are extending cyber protection in meaningful volume, even if the market is still in its early days. As a small and fairly new market, though, the cyber re/insurance sector needs to continue to evolve and mature. In doing so, it could certainly benefit from some more help. Reinsurance support has been crucial the expanding the breadth and depth of cyber insurance protection, but new sources of capital to address specific scenarios will provide the backbone for the next phase of industry growth.

The US national security strategy's reliance on the re/insurance industry represents a savvy approach to security, with the intent to support post-attack remediation in a manner that engages the expertise of the market and minimizes the impact to taxpayers. The global re/insurance industry has already demonstrated an appetite for cyber risk, and an ecosystem has begun to grow, to include reliance on new forms of capital like ILS. It is difficult to ignore the contrarians, though. Even if their views represent the minority, their underlying concerns represent an opportunity for the re/insurance industry market to show why it sees the cyber sector as robust and insurable. In addressing contrarian views directly, the result is a pervasive education that may, in the end, help attract further capital to the sector.

References

Artemis. (2024). *Insurance Linked Securities Investment Managers & Funds Directory*. Artemis. Retrieved 16 December 2023 from https://www.artemis.bm/ils-fund-managers/.

Artemis. (2024b). *Catastrophe Bond & Insurance-Linked Securities Deal Directory*. Artemis. Retrieved 16 December 2023 from https://www.artemis.bm/deal-directory/.

Artemis. (2016, April 27). *ILS & London can help cyber risk flourish – BNY Mellon*. Artemis. Retrieved 17 December 2023 from https://www.artemis.bm/news/ils-london-can-help-cyber-risk-insurance-flourish-bny-mellon/.

Artemis. (2015, September 14). *Cyber risk needs hybrid traditional & ILS reinsurance solutions: PwC*. Artemis. Retrieved 28 June 2023 from https://www.artemis.bm/news/cyber-risk-needs-hybrid-traditional-ils-reinsurance-solutions-pwc/.

ASTIN (2023, October 30). *7th ASTIN Cyber Workshop – A market set for growth* London: Lloyd's Old Library.

Baker, Tom and Anja Shortland. (2022). The government behind insurance governance: Lessons for ransomware. Regulation & Governance. Last revised 2023. Retrieved 17 December 2023 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4259411.

Beard, Stephen; Jim Sergent; and George Petras. (2021, August 30). *Aftermath of Ida: Millions without power along storm's devastating path*. USA Today. Retrieved 21 January 2024 from https://eu.usatoday.com/in-depth/graphics/2021/08/30/hurricane-ida-new-orleans-update-levee-damage-power-outage/5647202001/.

Biden, Joseph P. (2023, March). *National Cybersecurity Strategy*. Washington, D.C.

Biden, Joseph P. (2021. *Interim National Security Strategic Guidance* Washington, D.C.

Brantly, Aaron. (2020). Beyond Hyperbole. *The Cyber Defense Review,* 5(3), 99-120.

Braun, Alexander; Martin Eling; and Christoph Jaenicke. (2023). Cyber insurance-linked securities. *Astin Bulletin.* (53), 684-705.

Brew, Oliver. (20224, January 4). *Viewpoint: Scoring Cyber Insurance Predictions of 2023*. Insurance Journal. Retrieved 21 January 2024 from https://www.insurancejournal.com/news/national/2024/01/04/754341.htm.

Brooking, Emerson T. and Erica Lonergan. (2023, September 25). *Welcome to Cyber Realism: Parsing the 2023 Department of Defense Cyber Strategy*. War on the Rocks. Retrieved 17 December 2023 from https://warontherocks.com/2023/09/welcome-to-cyber-realism-parsing-the-2023-department-of-defense-cyber-strategy/.

Buchanan, Elizabeth. (2021, July 14). *Russia's 2021 National Security Strategy: Cool Change Forecasted for the Polar Regions*. RUSI. Retrieved 9 April 2022 fromhttps://rusi.org/explore-our-research/publications/commentary/russias-2021-national-security-strategy-cool-change-forecasted-polar-regions.

Bundt, Maya. (2021, Juney 10). *Cyber risk: Why we need a new approach to handling this explosive threat*. Swiss Re Blog. Retrieved 21 January 2024 from https://www.swissre.com/risk-knowledge/risk-perspectives-blog/cyber-risk-new-approach-to-threat.html.

Camillo, Mark. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*. 2(1), 53-63.

Carter, Rachel Anne; Darren Pain; and Julian Enoizi. (2002). *Insuring Hostile Cyber Activity: In search of sustainable solutions*. Zurich: Geneva Association.

Castriotta, Kelly and Sam Hansen. (2024, January 24). *Fact or Fiction: A Discussion on the Catastrophic Cyber Events Depicted in Leave the World Behind*. PLUS Blog. Retrieved 29 November 2024 from https://plusweb.org/news/fact-or-fiction-a-discussion-on-the-catastrophic-cyber-events-depicted-in-leave-the-world-behind/.

Cellerini, Elena Jelmini; James Finucane; Loic Lanci; and Thomas Holzheu. (2022, October). *Cyber insurance: strengthening resilience for the digital transformation*. Zurich: Swiss Re Institute.

Chung, Grace. (2021, June 10). *Global Investable Assets Reach Record $250 Trillion*. Institutional Investor. Retrieved 28 June 2023 from https://www.institutionalinvestor.com/article/2bswwcqa706wmg1zjrhfk/portfolio/global-investable-assets-reach-record-250-trillion?zephr_sso_ott=i80t0q.

Council on Foreign Relations (CFR). (2023). *Cyber Operations Tracker*. Council on Foreign Relations. Retrieved 17 December 2023 from https://www.cfr.org/cyber-operations/.

Din, Sajid Mohy Ul; Arpah Abu-Bakar, and Angappan Regupathi. (2017). Does insurance promote economic growth: A comparative study of developed and emerging/developing economies. *Cogent Economics & Finance*. 5, 1-12.

Eling, Martin and Werner Schnell. (2016). What do we know about cyber risk insurance. *Journal of Risk Finance*. Retrieved 13 March 2022 from https://www.emerald.com/insight/content/doi/10.1108/JRF-09-2016-0122/full/html.

Evans, Steve. (2020, October 7). *PCS launches Cyber RLM, a data tool for large insured cyber risks*. Artemis. Retrieved 21 January 2024 from https://www.artemis.bm/news/pcs-launches-cyber-rlm-a-data-tool-for-large-insured-cyber-risks/.

Evans, Steve. (2018, November 7). *Petya cyber industry loss passes $3bn driven by Merck & silent cyber: PCS*. Reinsurance News. Retrieved 21 January 2024 fromhttps://www.reinsurancene.ws/petya-cyber-industry-loss-passes-3bn-driven-by-merck-silent-cyber-pcs/.

Eyewitness News. 2023, August 14). *'From lights out to lights on': 20 years since the 2003 blackout*. abc7NY. Retrieved 17 December 2023 from https://abc7ny.com/2003-blackout-nyc-20-years-power-outage/13646160/.

Galeotti, Mark. (2021, July 5). *New National Security Strategy Is a Paranoid's Charter*. The Moscow Times. Retrieved 20 July 2022 from https://www.themoscowtimes.com/2021/07/05/new-national-security-strategy-is-a-paranoids-charter-a74424.

Gartzke, Erik. (2023, Fall). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*. 38(), 41-73.

Golling, Stefan. (2023, April 20). *War exclusions on the cyber market – Taking the next step*. Munich Re. Retrieved 17 December 2023 from https://www.munichre.com/en/insights/cyber/war-exclusions-on-the-cyber-market-taking-the-next-step.html.

Grant, Eric. (2020, September). *The Social and Economic Value of Insurance*. Geneva Association.

HM Government. (2020, March). Global Britain in a Competitive Age: The Integrated Review of Security, Defence, *Development and Foreign Policy* London.

Holmes, Aaron. (2022, August 22). *Companies Are Ditching Cybersecurity Insurance as Premiums Rise, Coverage Shrinks*. TheInformation. Retrieved 8 June 2023 from https://www.theinformation.com/articles/companies-are-ditching-cybersecurity-insurance-as-premiums-rise-coverage-shrinks.

Independent Cities Risk Management Authority (ICRMA). (No date given). *Earth Movement & Flood*. ICRMA.org. Retrieved 25 June 2023 from https://www.icrma.org/programs/insured/earth-movement-flood/.

Insurance Information Institute (I.I.I.). (2023). *Insurance for landslides and mudflow*. Insurance Information Institute. Retrieved 25 June 2023 from https://www.iii.org/article/insurance-for-landslides-and-mudflow.

International Association of Insurance Supervisors (IAIS). (2020, December). *Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development*.

International Union of Marine Insurance (IUMI). (2023, January 18). *11 months into the Ukraine war: Impact on global specialty lines*. IUMI. Retrieved 18 January 2023 from https://iumi.com/education/webinars/webinar-recordings-and-slides/11-months-into-the-ukraine-war-impact-on-global-specialty-lines_1683811237.

Johansmeyer, Tom. (2024, October 22). *The narrow case for cyber insurance backstops*. BindingHook. Retrieved 29 November 2024 from https://bindinghook.com/articles-binding-edge/the-narrow-case-for-cyber-insurance-backstops/.

Johansmeyer, Tom (2024b, June 25). *Cyber Attacks in Perspective: Cutting Through the Hyperbole*. Irregular Warfare Initiative. Retrieved 29 November 2024 from https://irregularwarfare.org/articles/cyber-attacks-in-perspective-cutting-through-the-hyperbole/.

Johansmeyer, Tom (2024c, August 23). Crowdstrike reveals a “small catastrophe” pattern in cyber insurance. BindingHook. Retrieved 29 November 2024 from https://bindinghook.com/articles-hooked-on-trends/crowdstrike-reveals-a-small-catastrophe-pattern-in-cyber-insurance/.

Johansmeyer, Tom (2023, November 15). *Is the Fear of Cyberwar Worse Than Cyberwar Itself?* Lawfare. Retrieved 16 December 2023 fromhttps://www.lawfaremedia.org/article/is-the-fear-of-cyberwar-worse-than-cyberwar-itself.

Johansmeyer, Tom. (2023b, June 27). *How Big Is the Cyber Insurance Market? Can It Keep Growing?*. Lawfare. Retrieved 28 June 2023 from https://www.lawfareblog.com/how-big-cyber-insurance-market-can-it-keep-growing.

Johansmeyer, Tom. (2023c). How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector. *International Journal of Security, Privacy and Trust Management*, 12(1), 1-14.

Johansmeyer, Tom and Alex Mican. (2022). Cyber ILS: How Acute Demand Could Drive a Scalable Retrocession Market. *Journal of Risk Management and Insurance*, 26(1), 40-59.

Kerman, Craig and Raymond Clouse. (2023, September). US Cyber Market Update: *2022 US Cyber Insurance Profits and Performance*. Aon.

Knake, Robert. (2016). *Creating a Federally Sponsored Cyber Insurance Program*.Council on Foreign Relations. Retrieved 21 January 2024 from https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program.

Lau, Sie Liang; Linda Sew; Paul Wee; and Jennifer Yong. (2020, August 6). *Cyber (Re)Insurance and ILS*. Singapore Actuarial Society (SAS) ERM Afternoon Talk. Retrieved 17 December 2023 from https://www.actuaries.org.sg/sites/default/files/2020-08/200806CyberReInsurance.pdf.

Lewis, James. (2020, August 17). *Dismissing Cyber Catastrophe*. Center for Strategic and International Studies. Retrieved 19 January 2024 from https://www.csis.org/analysis/dismissing-cyber-catastrophe.

Lloyd's. (2015, May). *Business Blackout: The insurance implications of a cyber attack on the US power grid*. London: Lloyd's.

Lostri, Eugenia; James Lewis; and Georgia Wood. (2022, March 22). *A Shared Responsibility: Public-Private Cooperation for Cybersecurity*. Center for Strategic and International Studies. Retrieved 21 January 2024 from https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

Mukhopadhyay, Akankshita. (2023, June 26). *Europe poised to lead in addressing evolving cyber risks: FERMA*. Reinsurance News. Retrieved 16 December 2023 from https://www.reinsurancene.ws/europe-poised-to-lead-in-addressing-evolving-cyber-risks-ferma/.

National Association of Insurance Commissioners (NAIC). (2022, October 21). *NAIC Report Shows Premiums Grew 61% as Cyberthreats Rose in 2021*. Retrieved 17 December 2023 from https://content.naic.org/article/naic-report-shows-premiums-grew-61-cyberthreats-rose-2021.

Newman, Ian; Ed Pocock; and Jemima Hall. (2022). *Cy-Fi: The Future of Cyber (Re)insurance*. London: Gallagher Re.

Olson, David. (2016, November 9). *Insurance as a Social Good*. Wisconsin School of Business. Retrieved 17 December 2023 from https://business.wisc.edu/faculty-research/risk-insurance/blog/insurance-as-a-social-good/.

Pain, Darren. (2023, November). *Cyber Risk Accumulation: Fully tackling the insurability challenge*. Zurich: Geneva Association.

Parsoire, Didier and Sebastien Heon. (2016, September 30). *Cyber Risks on the Rise*. SCOR Global P&C Annual Conference. Paris. Retrieved 17 December 2023 from https://www.scor.com/sites/default/files/04_didierparsoire_sebastienheon.pdf.

Przetacznik, Jakub and Simona Tarpova. (2022, June). *Russia's War on Ukraine: Timeline of cyber-attacks*. European Parliamentary Research Service. Retrieved 21 January 2024 from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Rid, Thomas. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(2), 5-32.

Russian Federation. (2021). National Security Strategy. Retrieved 18 July 2022 from https://acrobat.adobe.com/link/review?uri=urn:aaid:scds:US:438ab784-5cb3-409f-b6bc-920eee9a30bb#pageNum=1.

Smeets, Max. 2018). The Strategic Promise of Offensive Cyber Weapons. *Strategic Studies Quarterly*, 123,: 90-113.

Staguhn, Janina and Romina Bandura. (2023, May 5). *Insurance as a Critical Enabler for Investing in Ukraine*. Center for Strategic and International Studies. Retrieved 17 December 2023 from https://www.csis.org/analysis/insurance-critical-enabler-investing-ukraine.

Stark, Tim. (2021, August 23). *Cyber insurance market encounters 'crisis moment' as ransomware costs pile up*. CyberScoop. Retrieved 23 August 2021 from https://cyberscoop.com/cyber-insurance-ransomware-crisis/.

Ukraine. (2020, September 14). *National Security Strategy of Ukraine*. Retrieved 21 January 2024 from https://zakon.rada.gov.ua/laws/show/392/2020#n2.

Ukraine. (2017, August 18). *Energy Strategy of Ukraine for the Period up to 2035: 'Security Energy Efficiency, Competitiveness*. Kyiv: Cabinet of Ministers of Ukraine.

Waldrop, Theresa. (2021, September 8). *Hurricane Ida took down more power poles in 2 states than Katrina, Ike, Delta and Zeta combined, power company says*. CNN. Retrieved 21 January 2024 from https://edition.cnn.com/2021/09/07/us/hurricane-ida-aftermath-louisiana-tuesday/index.html.

Wilde, Gavin. (2022, December 12). *Cyber Operations in Ukraine: Russia's Unmet Expectations*. Carnegie Endowment for International Peace. Retrieved 21 January 2024 from https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

Woods, Daniel and Andrew Simpson. (2017). Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, 2(2), 209-226.