Proceedings of the 2025 Winter Simulation Conference
E. Azar, A. Djanatliev, A. Harper, C. Kogler, and V. Ramamohan, eds.

SUSTAINING CAPITAL-BOOSTED CYBER REINSURANCE MARKETS USING CAT BONDS

Ranjan Pal[1], Bodhibrata Nag[2], Sander Zeijlemaker[1], and Michael Siegel[1]

[1]MIT Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, USA
[2]Operations Management Group, Indian Institute of Management Calcutta, INDIA

ABSTRACT

Cyber insurance (CI) markets improve the cybersecurity of companies (enterprises) in theory. This theory is increasingly being validated in practice in multiple enterprises that buy cyber insurance. However, the supply-demand gap in the CI market is huge and stretches over a trillion dollars. The primary reason being that cyber reinsurance companies do not have sufficient capital to serve their CI company clients through profitable cyber-risk portfolio diversification. This capital problem is subsequently rooted in the fundamental challenge of enterprise cyber posture information asymmetry that has plagued the CI industry since its inception. A radical capital-boosting mechanism proposed by researchers and deployed within the industry in the last two years is an insurance-linked security (ILS) product such as a catastrophic (CAT) bond. In this paper, we present arguments on *why*, *how*, and *when* CAT bonds help sustain capital-boosted reinsurance markets complemented by innovative AI/ML-driven inside-out cyber posture scanning solutions.

1 INTRODUCTION

Digitally driven enterprise supply chains are becoming increasingly widespread. Popular examples include enterprise supply chains supported by critical infrastructure, such as the power grid and cloud systems (see Figure 1). While the modern power grid built upon a cyber-physical system supports virtually all societal enterprise sectors, the cloud systems supporting SaaS, PaaS, and the IaaS service paradigms are the backbone of nearly every business today. Consequently, a service disrupting cyber attack (or system configuration-induced reliability faults) on such critical infrastructures will simultaneously cripple/disrupt the services offered by enterprises on a supply chain in a systemic fashion and increase business risk (of service discontinuity). The business risk arising from such attacks is often termed a systemic cyber risk.

Some leaders of the annual World Economic Forum (WEF) meet of 2023 projected that geopolitical instability around the world will most likely result in cyber attacks on critical infrastructure in the near future that will result in an increase in systemic business risk events of significant adverse impact. Examples of such attacks in the recent past include (i) the *Log4j* attack (2021) exploiting *Log4Shell* as a zero-day vulnerability in the low-profile Log4j software utility embedded in billions of enterprise devices, (ii) the *SolarWinds* cyber incident (2020) exploiting malicious trojan code (*Sunburst*) into the software update of IT performance management system *Orion* to gain access to confidential business workflow information of more than 18,000 enterprises, (iii) the *Colonial Pipeline* ransomware-flavored cyber attack (2021) that forced the company to close down business operations on 5500 miles of the US East Coast for a week, and (iv) the *NotPetya* cyber attack that took advantage of two known exploits in older Windows versions: *EternalBlue* and *Mimikatz* to embed malware into a tax filing software application used by multiple enterprises, and resulted in shutdowns and took days to resume normal functionality. Many of such cyber attacks cost multi-billion USD to society and the global economy.

1.1 Cyber Insurance to Mitigate (Systemic) Risk Impact and Improve Cybersecurity

Most of such (if not all) business disruption incidents cost national economies hundreds of millions (if not billions) of dollars, and most of these costs till date are absorbed by affected enterprises on the digital

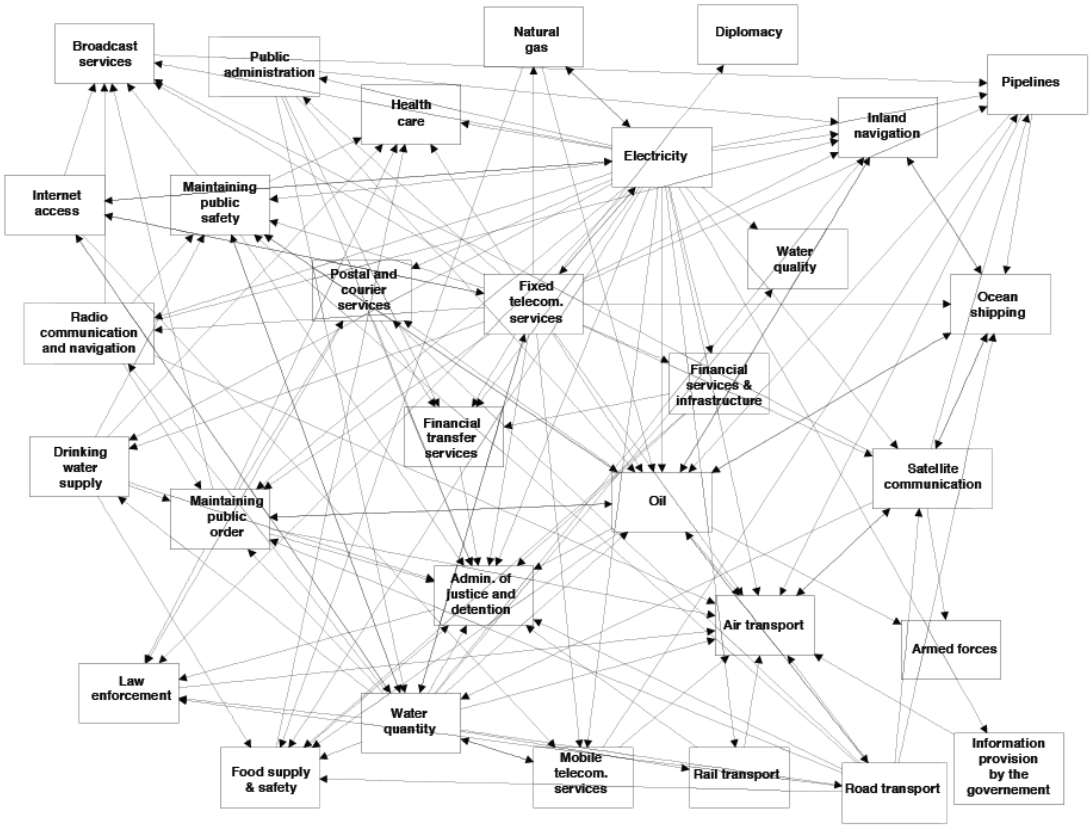

Figure 1: Showcasing the chart of complex service dependencies among networked enterprise sectors with critical cyber infrastructure. [*Source:* Netherlands Organization for Applied Scientific Research (TNO)].

supply chain. One might argue that cyber risk transfer tools such as insurance can cover much of such costs, parallel to that in traditional risk management scenarios.

The concept of cyber insurance (CI) here, for the uninitiated, is that enterprises transfer residual cyber risk to insurance companies in return for insurance premiums. Residual cyber risk is that portion of a post cyber incident risk that businesses (enterprises) cannot manage through traditional risk management tools such as vendor products (e.g., anti-virus, firewalls, other security controls like zero trust mechanisms and multi-factor authentication) and self-insurance (reserving a monetary organizational budget for post cyber breach incident response). Examples of popular cyber (re-)insurance providers include *AIG, Lloyds, Beazley, FM Global, SCOR, Munich Re*, and *Zurich*.

The additional encouraging thing regarding cyber insurance is that it improves cybersecurity of enterprises and their inter-networked ecosystems. This has been mathematically proven in multiple papers over the last decade using methodologies from economics and computer science (Lelarge and Bolot 2009; Shetty et al. 2010; Pal and Golubchik 2010; Pal et al. 2011; Pal et al. 2014; Pal et al. 2018; Khalili et al. 2018), and is currently being validated in practice. The cyber analytics firm *NetDiligence* surveyed around 540 decision makers from approximately 500 small and medium businesses (SMBs) and most of them had evidence that cybersecurity and cyber resilience improved in their firms post them buying standalone cyber insurance. The basic insight here is that CI acts as a control mechanism for enterprises to improve their cyber posture without which they may not get the desired coverage from insurance companies - in the worst case, may not even be insured. As an example, 45% of digitally run businesses in Canada could not renew their cyber insurance contracts in 2023 due to not achieving cyber posture benchmarks set by the

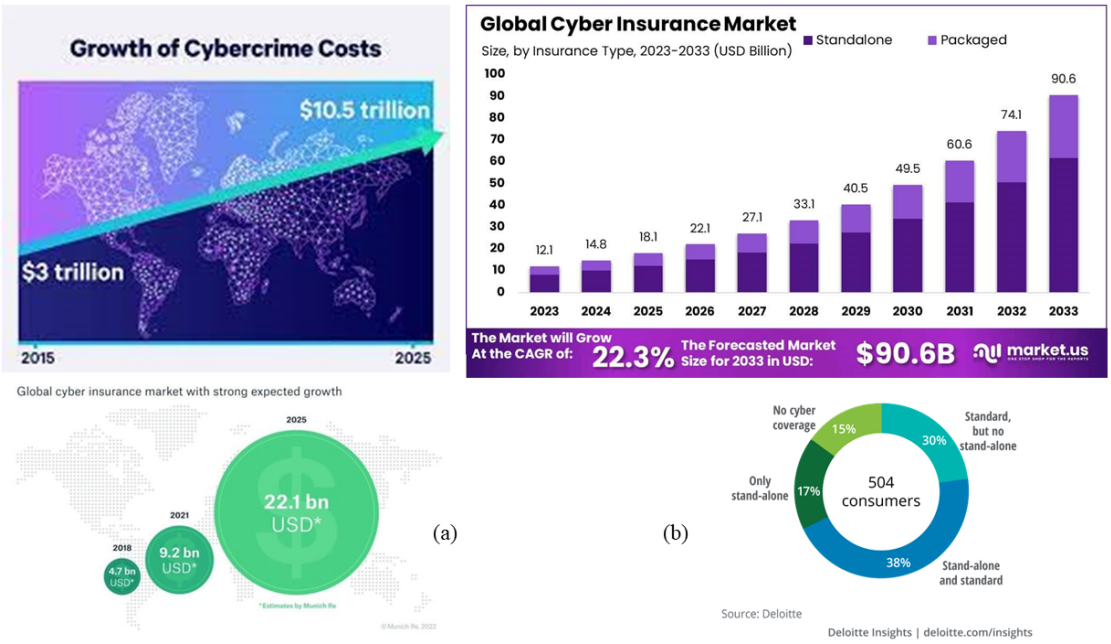

Figure 2: Showcasing (a) the sparse CI market relative to global cyber crime losses [*Source:* Munich Re], (b) a much larger mixed CI market when compared to a standalone CI market [*Source:* market.us, Deloitte]

.

insurers. According to *Gallagher Re*, certain CI carriers denied ransomware claims from enterprise clients globally who had open RDP ports (a popular entry point for ransomware attacks) in their IT systems.

1.2 The Strange Case and Reasons for Sparse Cyber Insurance Markets

It is prudent of most enterprises (if not all) to invest in sufficient cyber insurance simply because the cyber vulnerability terrain is too large and too uncertain, i.e., too many known unknowns and unknown unknowns, for risk officers in any enterprise to anticipate every cyber attack and its possible (multi-party) impact on the enterprise. As a matter of fact, eliciting the number of cyber vulnerabilities in any system is NP-hard (Pal et al. 2023; Pal et al. 2021) and a Turing undecidable problem (Pfleeger and Cunningham 2010) in theoretical computer science. In other words, leave alone humans, even the world's most powerful computers will find it difficult to elicit in finite time the number of ways a hacker can breach the system. Hence, it is wise to invest in covering residual cyber risk. Moreover, there is never enough cybersecurity budget for nearly every business to prevent all possible attack scenarios that an enterprise cyber risk management team might envision/anticipate.

In practice, cyber insurance markets to cover residual cyber risk are worth around 25 billion USD in capital, with most enterprises today buying some degree of cyber insurance. Most of such capital (nearly 50%) are sourced from cyber reinsurance companies that are far fewer in number than the cyber insurance companies. However, the global costs of cyber crime run in trillions of USD. Hence, it is strange that with most enterprises willing to invest in CI, the supply-demand gap is very high (see Figure 2). The primary cause here is that most enterprises who invest in cyber insurance do not invest purely in standalone cyber insurance (Firms *Forrester, market.us, Deloitte* estimated this number to be around 15% in 2023). This is true mostly of SMBs who form 80% of the global businesses and enterprise supply chains. It is standalone (and not traditional/mixed) CI that has been empirically validated in certain enterprises to improve cybersecurity. Hence, its important to reason *why enterprises don't buy sufficient standalone CI.*

The underlying reasons (discussed with cyber insurers and enterprise risk officers affiliated with MIT CAMS) for multiple cyber insurers being in business but very few selling standalone policies are; (i) lack of sufficient enterprise cyber posture information exchange between businesses and insurance companies (or between businesses and public) that does not provide enough confidence to the latter to price and underwrite competitive and client-attractive policies in the systemic cyber risk era, (ii) unattractive standalone policy pricing and very long questionnaires pushing enterprises to buy coverage that is merged with non-standalone cyber insurance - such coverage policies have high insurance loss ratios, and (iii) upper management and board, though risk averse, are behaviorally induced to under estimate the degree of cyber risk their enterprise is exposed that subsequently leads to them investing in standalone cyber insurance policies, and (iv) a lack of sufficient ability of cyber insurers to bring CISOs and CROs of enterprises to talk in the same language in terms of quantifiable cyber risk impact.

1.3 The Advent of Insurance-Linked Securities to Scale Standalone CI Markets

The sparse but steadily growing (standalone) cyber insurance market implies an important but worrying fact (mentioned in a 2023 WEF meeting): *if there is a low (but growing) chance event that a major critical infrastructure like a power grid in a big city is taken down for half a day by cyber adversaries, the cyber insurers and reinsurers will be exposed to a systemic business loss coverage demand in billions of USD that is far more than their capacity for a given time and geography.* This is because several businesses (within and across local geographies) reliant on an uninterrupted power supply (see Figure 1) would suffer from business disruption at the same time. In such a catastrophic scenario, the society has to bear the cost of adverse socio-economic impact, simply because there is not enough insurance capital to cover cyber events of such impact magnitude. Even if we account for some recent market studies by *Fitch Ratings* that standalone cyber coverage is increasing by the year, the capital inflow is not significant for the cyber (re)insurance market to stand alone to manage modern cyber risk. *If one could design an alternative cyber risk transfer mechanism for worst-case cyber attack scenarios, it would not only allow the better response and recovery from catastrophic impact, but would also find it much easier to cover at scale non-catastrophic cyber incidents that are far more commonplace by supplementing cyber (re)insurance solutions.* After all, *Gallagher Re* projects CI claims to overtake the most dominant property insurance claims, by 2040. Hence, alternative risk transfer markets will be needed that can be sustainable to manage such claims.

We envision that the practice of an increasing number of cyber reinsurance companies selling catastrophe bonds to financial investors (e.g., hedge fund companies) in the form of insurance-linked securities (ILSs) in return for significant capital inflow, will help the current cyber (re)insurance industry to effectively handle catastrophic and correlated cyber event impact coverage (Cummins and Trainar 2009). This is because (systemic) cyber losses worth billions of USD from a single cyber event are diversified/traded in the multi-trillion (approximately 40 trillion USD currently) financial markets, and will provide significant steady returns to the investors. This will subsequently hand more capital to cyber (re)insurance businesses and densify these markets in terms of sold standalone CI policies (under conditions we will cover later in the paper). The idea of ILSs as an alternative risk transfer mechanism has been in operation since the *Hurricane Andrew* natural catastrophe event in 1992, where reinsurance companies sold catastrophe (CAT) bonds to investors in return for capital to cover natural CAT risks. The same idea has been transformed in the cyber space in practical reality through the introduction of the world's first cyber CAT bond announced by *Beazley* in January 2023 (and a few more in 2023 and 2024) with the goal to create a scalable market boosting the standalone cyber (re)insurance business.

1.4 Motivation and Paper Contributions

In this paper, we are motivated to study *if, how,* and *when* capital boosting insurance-linked security products (such as CAT bonds) can scale cyber (re)insurance markets to close the big supply-demand gap in these

markets. Hopefully, a gap reduction would significantly scale (standalone) CI markets and boost enterprise cybersecurity. Consequently, we make the following contributions in this paper.

- We provide a logical, structural, and intuitive explanation on how CAT bonds (an example of an ILS product) can be used to boost capital in cyber (re)insurance markets (see Section 3).
- We propose a detailed outline of a data-driven market model to analyze the success (or otherwise) of CAT bond products to boost cyber (re)insurance markets as a function of the amount of cyber posture information reinsurers have about the the portfolio of cyber risks their cyber insurer clients are exposed to. We ideate on how simulations driven by modern AI can enable cyber reinsurers to estimate such information (see Section 4).
- We showcase analysis results from our proposed data-driven market model to characterize equilibrium conditions (matching theory and simulations) under which cyber insurers would find it economically sustainable to (a) only invest in retaining cyber risk of their enterprise clients, (b) transfer their risk to reinsurance companies, or (c) transfer their risk using a combination of reinsurance and CAT bonds (see Sections 4 and 5).
- We discuss the implications of the results on improving ILS-driven CI markets using AI/ML ops, and enterprise cybersecurity via the NIST framework, and propose implementable action items for stakeholders of the CAT bond catalyzed cyber (re)insurance markets to realize in practice the model results in theory that promote sustainable capital injection into CI markets (see Sections 5 and 6).

We discuss related work in Section 2, and conclude in Section 7.

2 RELATED WORK

In this section, we briefly review research related to residual cyber risk management markets.

Cyber Insurance to Improve Cybersecurity - It is only because of the inherent potential of cyber insurance to improve enterprise security governance that we have a market for third-party (systemic) risk transfer. This proven potential of cyber-insurance to improve cybersecurity has been mathematically shown in seminal papers (Lelarge and Bolot 2009; Shetty et al. 2010; Hofmann 2007; Pal and Golubchik 2010; Pal et al. 2014; Naghizadeh and Liu 2014; Pal et al. 2018; Pal et al. 2011; Pal et al. 2017; Yang and Lui 2014). In practice, cyber insurance markets have steadily seen an increase over the years (specifically, since the last decade and a half) with cyber insurance solutions demanding sufficient cybersecurity controls on part of enterprise clients to be contract-eligible, or receive significant coverage. This consequently supports these enterprises to effectively adapt, absorb, and respond to cyber incidents. The readers are referred to (Dambra et al. 2020; Marotta et al. 2017) for a review of the role of cyber insurance.

Methodologies to Manage Systemic Cyber-Risk - Systemic cyber risk management is one of the major applications feeding into CI markets. The authors in (Pal et al. 2023; Pal et al. 2021; Pal et al. 2024) have shown that optimally estimating and diversifying systemic cyber risk (an integral insurance operation to manage a portfolio of cyber risks) is NP-hard. However, the hardness of optimally estimating and diversifying (systemic) cyber-risk does not deter the existence of non-optimal but diversification sustainable portfolios of (systemic) cyber risk for cyber re-insurers. Recent theoretical efforts investigated the diversification sustainability problem for i.i.d. cyber risk portfolios. In a series of efforts (Pal et al. 2020; Pal et al. 2020; Pal et al. 2020; Pal et al. 2023; Pal et al. 2021), the authors have proved that diversifying a portfolio of *catastrophic* heavy-tailed cyber risks (each having infinite mean and potentially sourced from individual risks from multiple enterprises) that are identical and independently distributed (i.i.d.), i.e., not tail-dependent, *is not* an effective economically sustainable practice for reinsurers with respect to the industry-popular Value-at-Risk (VaR) tail risk measure. On the other hand, diversifying a portfolio of i.i.d. heavy-tailed cyber risks that are *not catastrophic* (risks with finite mean and sourced from individual risks from multiple enterprises) is economically sustainable for reinsurers. However, (systemic) cyber risks are often generated from non i.i.d. individual enterprise cyber risk sources. In (Pal et al.

2024; Pal et al. 2025), the authors derive the conditions for economic sustainability of systemic cyber risk portfolio diversification when such portfolios that cyber re-insurers are exposed to, consist of non i.i.d. risks with arbitrary tail nature. The authors in (Pal et al. 2023; Pal and Nag 2024) propose models on market efficiency of ILS-driven CI markets and their pricing, respectively - however, they do not propose a decision science as to when it is suitable for CI companies to (a) only invest in retaining cyber risk of their enterprise clients, (b) transfer their risk to reinsurance companies, and (c) transfer their risk using a combination of reinsurance and CAT bonds. This is the main decision problem for the CI industry.

3 HOW CAN CAT BONDS DENSIFY CYBER INSURANCE MARKETS?

As mentioned earlier, current CI markets lack sufficient capital for cyber insurance and reinsurance businesses to profitably diversify their (systemic) risk portfolios that can comprise of many correlated cyber risks. The authors in (Pal et al. 2024; Pal et al. 2025; Pal et al. 2021) have recently shown that the Value-at-Risk (VaR) on diversification of such portfolios increases with the size of the portfolio. This implies that unless cyber reinsurers have a sufficient capital buffer, high premiums charged to clients (insurance companies who further offload it to enterprise clients) is the only way to keep cyber (re)insurance markets economically sustainable. This is a reason why many enterprises, particularly the SMBs, opt out of purchasing cyber insurance. In other words, the lack of sufficient capital primarily leads to dampening demand that further constricts CI supply and leads to CI market failure in general.

The big question at hand then becomes: is there a way to boost capital injection in CI markets that improves demand and increases supply? *Insurance linked security (ILS) solutions such as catastrophe (CAT) bonds might just provide an answer to this all important question.* In this section, we first provide the working logic behind (cyber) CAT bonds boosting capital injected into cyber (re)insurance markets. We then follow up with the basics (for the general reader) of the functioning mechanism behind CAT bonds.

Logic Behind Boosting Capital in Cyber (Re)Insurance Markets - The crux behind the potential effectiveness of ILS solutions such as CAT bonds is that their markets rely on special purpose vehicles (e.g., Goldman Sachs) working with cyber reinsurance firms and trading investor capital driven securities in the relatively less cyber-correlated multi-trillion financial markets. Since financial markets can draw on larger, more liquid, and increasingly diversified pool of capital than the equity of cyber (re-)insurance markets, diversifying (at most) a few hundred billion dollars of cyber-risk in a 30-odd trillion dollar financial market is akin to insuring a *drop in an ocean*. According to a *Hannover Re* (a global leader in providing re-insurance services) report, the ILS market is approximately worth USD 100 billion. Even though this is not near to being a trillion dollar market, it is high enough to improve the density of current CI markets in terms of sold (standalone) cyber insurance policies. Subsequently, this will also improve the ILS market with more steady returns for investors churned out of increased capital investments in an increased number of CI policies. In relation to reinsurance solutions necessarily needing to complement with ILS products to manage residual and systemic cyber risk, according to risk data analytics firm *Verisk*, *"many insurers are not able to get all the protection they want, even on reinsurance rate increases of up to 50%, which itself represents acceleration from the July 1, 2021, reinsurance renewal's increases of 40%. Further, many reinsurers struggle with capacity, given a lack of access to retrocession, which would require new sources of capital (e.g., through ILSs), given the concentration risk observed in the cyber reinsurance sector."* Having discussed the logic of ILSs behind boosting cyber (re)insurance capital, we touch upon the basic functionality of ILS solutions such as CAT bonds, as applicable in cyber settings.

How Do CAT Bonds Function? – CAT bonds when compared to treasury and municipal bonds are only triggered in the event of a catastrophe – characterized by a (cyber) loss value above a particular high threshold (e.g., above USD 400 million in cyber loss settings). Such bonds are useful to not only manage CAT cyber risks such as the one mentioned in the WEF meeting in 2023 (see Section 1.4), but as a byproduct can be easily applicable to manage non-CAT cyber risks. In the context of cyber, when a trigger event such as a 'rare' catastrophe occurs (e.g., a critical manufacturing/power plant shuts down for hours/days at a stretch) within a bond term (e.g., two years), the bond sponsor (the cyber insurer paying loaded premiums

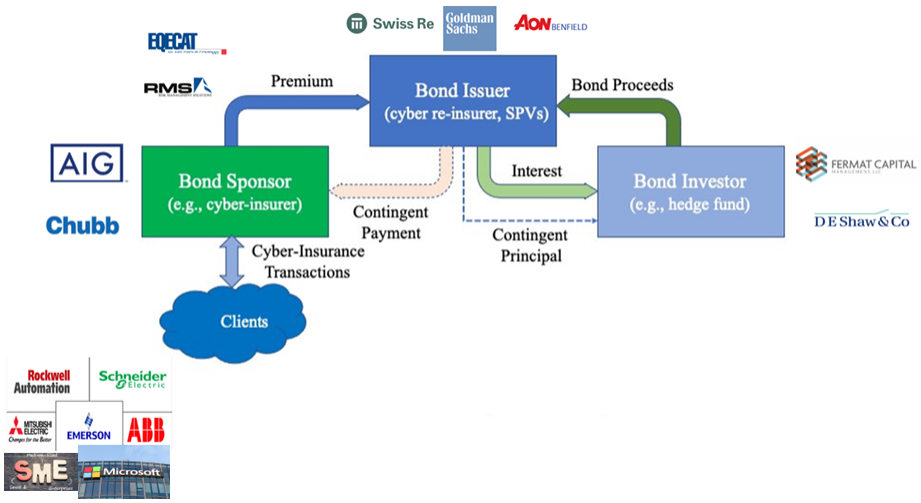

Figure 3: An illustration of a catastrophic (CAT) bond functionality with market stakeholder examples.

to a bond issuer) keeps a portion of the bond value to pay off aggregate first and third party cyber losses. The investors (e.g., hedge funds) on the other hand lose some or all of their principal (capital) invested. The bond issuer (e.g., cyber reinsurance firm along with special purpose vehicles and/or investment banks) creates the bond and pays, as return of investment (ROI) for the investor, a sum of interest (based on market rates) after collecting premiums from the bond sponsor and loaded premiums from trading bond proceeds in the financial market. If the catastrophic cyber event does not occur during the bond term, the investors get their invested capital back at a maturity date. The feasible maturity period of a contract can be anywhere between one year to 10 years. As an example, the first Beazley CAT bond had a contract maturity period of one year. Usually, a larger period contract helps cyber (re)insurers manage the adverse impact from a low-frequency cyber incident with large spillover effect (e.g., the *NotPetya* cyber incident). The functioning mechanism of financial CAT bonds is illustrated in Figure 3.

4 A DATA-DRIVEN ILS-DRIVEN CYBER (RE)INSURANCE MARKET MODEL

We consider the scenario where a cyber (re)insurer has a capital amount C that is reserved to cover a portfolio of (multiparty) enterprise cyber risk distributions. This portfolio can either be handled by an insurer or reinsurer for the purpose of diversification. In the cyber world, risk portfolios are frequently handled by reinsurers (alongside insurers) as (a) they inject more than 50% of capital in the CI business, and (b) are increasingly exposed to systemic risk coverage claims.

We assume that a cyber loss incident occurs for which, with probability p (the portfolio risk in this model), the (re)insurer needs to payout an amount A such that $C - A < 0$. Alternatively, this situation reflects that the (re)insurer does not have sufficient capital to cover impact of a cyber attack. We assume that the (re)insurer adverse selection problem exists in the sense that the (re)insurer has relatively more (if not perfect) information about the enterprise cyber posture risk contributing to a portfolio than any other entity (apart from the enterprise). The current CI market has access to AI/ML ops driven invasive solutions that can provide robust estimates of enterprise cyber posture. Examples such products are sold by *Bitsight*, and *SAFE Security* that provide estimates of probability p to cyber (re)insurance firms. As part of simulation exercise to validate our model theory, we vary the uncertainty around the estimated value of p (as a proxy to insurance information asymmetry) through a light-tailed statistical distribution.

The question the paper wants to address is: *under what conditions will the cyber (re)insurer resort to (a) reinsure the portfolio risk in question, (b) retain or self-insure the portfolio risk, and (c) resort to ILS products such as a CAT bond to manage the portfolio risk.*

When is Cyber Reinsurance a Viable Risk Transfer Option? - It is obvious that for a (re)insurer would reinsure, the optimal contract will solve the following optimization problem:

$$\max_{PR_r(p),PO_r(p)} (C+PR-PR_r(p))(1-p)+(C-A-PR_r(p)+PO_r(p))p-CR\cdot p\cdot \mathbb{1}_{\{PO_r(p)<A+PR_r(p)-W\}},$$

where PR is the net premium the (re)insurer gets from policies it underwrites for its enterprise clients, $PR_r(p)$ is the premium it pays to a cyber reinsurer to cover residual portfolio risk it does not have capital for, $PO_r(p)$ is the contingent payout of the cyber reinsurer to the (re)insurer to cover the latter's residual portfolio risk, CR is the transactional cost that the (re)insurer needs to pay to transact in cyber reinsurance, and $PR_r(p) \geq (1+\delta)\cdot pPO_r(p)$ with $pPO_r(p)$ being the actuarially fair cyber reinsurance premium, and δ being the loading factor atop the premium. An algebra workaround this optimization problem results in a (re)insurer choosing self-insurance if $p > \frac{CR-(A-C)\delta}{CR(1+\delta)}$ (as profit maximizing reinsurers will not offer a contract for $p > \frac{1}{1+\delta}$), and opts for cyber reinsurance otherwise to manage its portfolio of enterprise cyber risk. This analysis results in the optimal cyber reinsurance to have the parameters: $PR_r(p) = \frac{(A-C)p(1+\delta)}{1-p(1+\delta)}$, as reinsurance premium (increasing in p) and $PO_r(p) = \frac{A-C}{1-p(1+\delta)}$ as the contingent reinsurance payout (excess of loss) to a cyber (re)insurer.

When is CAT Bond Securitization a Viable Risk Transfer Option? - The biggest challenge for CAT bond investors is information asymmetry (IA) in the form of adverse selection on enterprise cyber posture information and loss probability p. The cyber reinsurers have more information on this, and they will deal with such information strategically (also keeping regulation-promoting privacy interests in mind) while contracting with CAT bond investors. This brings us to a microeconomic signaling game (of incomplete information about p) setting . Say there is a cyber posture information index I underlying the reinsurer portfolio relevant to an index-triggered CAT bond contract (PR_{index}, PO_{index}). Given the CR_{bond} - the transactional cost that reinsurer pays to get a CAT bond contract is fixed, $PR_{index} = \frac{q}{1-q}(A-C)$, and $PO_{index} = (A-C)+PR_{index}$ (because premiums are fair due to known q), implying full coverage from a CAT bond contract is the optimal demand for a cyber reinsurer. Here q is the probability of reduction in I (information known to investor, and obtained using invasive AI/ML ops) The expected cost of the contract to the reinsurer is the sum of the expected benefit/cost of the index contract premium, and the expected cost of basis risk, and equals $\left(\frac{q}{1-q}-\frac{p}{1-p}\right)(A-C)+(p-q)_+CR_{bond}$, where p is the portfolio risk for a cyber (re)insurer. This expression decreases in p when $1-\sqrt{\frac{A-C}{CR_{bond}}} < p < q$, and increases when $q < p < 1-\sqrt{\frac{A-C}{CR_{bond}}}$. This expression is zero when basis risk is zero in ideality.

Monte Carlo Simulation of Theory - We play the signaling game of incomplete information using a Monte Carlo simulation by randomizing p (via light and heavy-tailed distributions) and q (via a light-tailed distribution) to simulate a market perfect Bayesian equilibrium (PBE) indicating when reinsurance/securitization (CAT bonds)/self-insurance is the best action for a reinsurer to manage cyber risk.

5 MODEL SIMULATION OUTCOMES AND MARKET ECOSYSTEM IMPLICATIONS

In this section we describe the results of our analysis in three parts. We first analyse our Monte Carlo simulations results for our proposed market theory in Section 4 to showcase CAT bond induced CI market sustainability conditions. We then showcase the vital role of data science (AI/ML ops) in boosting the CAT bond driven CI market ecosystem. Finally, we discuss how stakeholders in this ecosystem can satisfy the NIST cybersecurity framework principles, given cybersecurity being the main vision of CI markets.

Market Sustainability Conditions - We observe from Figure 4(a) that there are zones (blue, green, orange) as a function of information asymmetry (IA that ranges from 0 to $IA_{\max}$ and a function of p and q in Section 4) within which cyber reinsurance only, cyber reinsurance with securitization via CAT bonds, and self-insurance are optimal decisions by CI businesses transferring residual cyber risk of their clients to

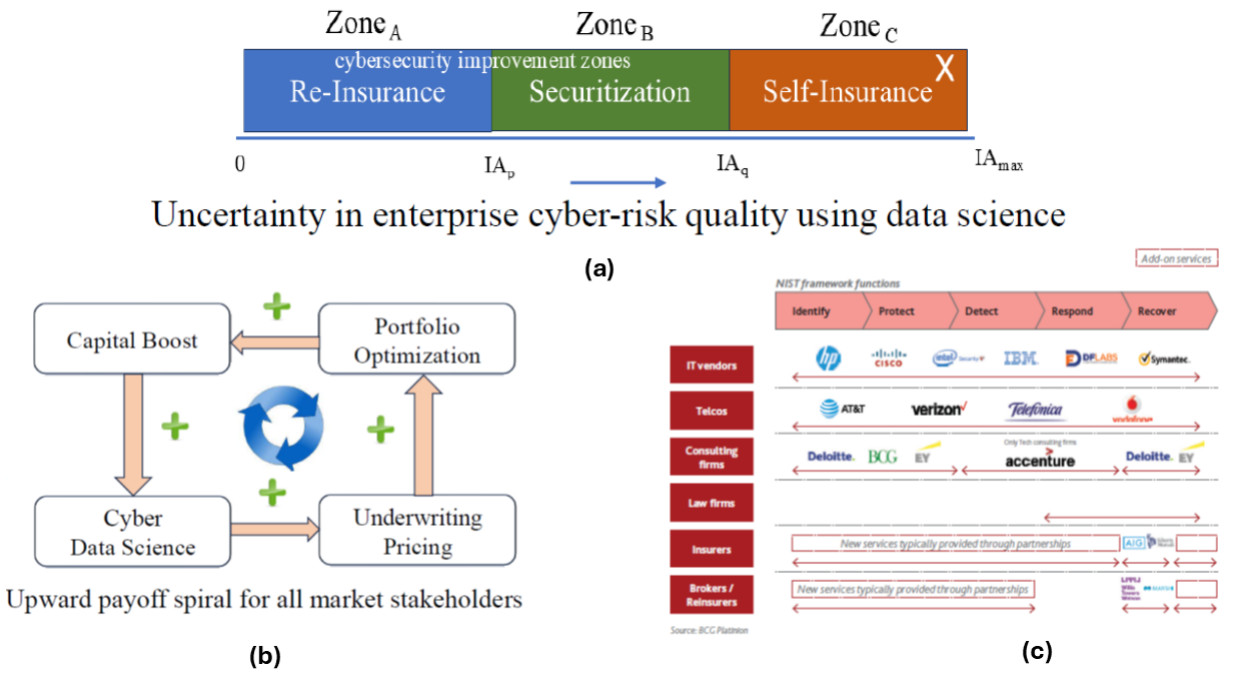

Figure 4: An illustration of model simulation outcomes and market ecosystem implications.

cyber reinsurers. The blue and green zones are likely to increase sale of standalone CI policies that improve enterprise cybersecurity. The interesting thing to understand is that securitization is a market equilibrium decision when IA lies between intermediate values IA_p and IA_q (here p and q not related to p,q in Section 4). Alternatively, due to the risk averse nature of profit-minded CAT bond investors there is an upper bound of IA beyond which they do not find it incentive compatible to invest. Note here that high IA does not mean very high impact risk (after all the entire purpose of CAT bonds is to hedge very high impact cyber risk outcomes). What investors care about is high statistical confidence about the estimates of very high impact risk. Low confidence signal high ILS basis risk/transaction costs and vice versa. This confidence is significantly lower in cyber environments than in natural (nat) CAT environments. Hence, the green zone is not as large for CAT-bond driven CI markets when compared to nat-CAT (e.g., hurricane) markets where historical data and physics modeling increase the statistical confidence. In addition, ILS markets for cyber are usually index triggers that in theory increase basis risk (Braun 2016).

The Role of Data Science to Boost ILS-driven Ecosystems - The crux step in Figure 4(b) is 'cyber data science'. A capital boost by CAT bond investors will only be sustainable if cyber risk modelers can leverage the power of AI/ML ops to much reduce the IA in relation to cyber risk portfolio sourcing from CI client enterprise cyber posture. This would need ecosystem stakeholder action items that we discuss in Section 6. On the other hand, capital boosted (re)insurers can invest in more effective invasive AI/ML ops to accurately estimate portfolio cyber risk portfolios. A capital boost and effective AI/ML cyber posture estimation processes in place improves underwriting and pricing of CI contracts increasing the chances of selling of more (standalone) CI policies. With more contracts sold, there is more cyber risk profile data to optimize portfolio diversification by cyber reinsurers, that eventually results in additional capital boost, closing the loop in Figure 4(b) on an upward spiral, and boosting the ILS-driven CI market ecosystem.

An ILS-driven CI Ecosystem Value Chain Influencing the NIST Cybersecurity Framework - The vision of CI markets is to improve enterprise (ecosystem) cybersecurity. One standard adopted industry wide towards better cybersecurity is the NIST framework. This framework consists of five steps: *identify, protect, detect, respond,* and *recover*. The ILS-driven CI market ecosystem should influence all these five

steps of the NIST framework to ensure the CI vision is on the right path. We at MIT CAMS worked with the *Boston Consulting Group* (BCG) who provided us with the *BCG Platinion* framework for this purpose. The framework consists, in one dimension of the matrix in Figure 4(c), of CI ecosystem stakeholders including (but not limited to) IT vendors, telcos, consulting firms, law firms, insurers, and reinsurers/ILS investors/risk modelers. On the other dimension of the matrix are the five pillars of the NIST framework that are influenced by the multiple stakeholders. Given the results obtained via theory and simulations, the (re)insurers, ILS investors, and the cyber risk modelers need to use AI/ML ops services by other value chain stakeholders (e.g., by IT vendors, third parties) to improve the performance of the NIST cybersecurity pillars, and broaden the green and blue zones in Figure 4(a).

6 ACTION ITEMS FOR ILS-DRIVEN CYBER INSURANCE MARKET STAKEHOLDERS

In this section, we propose implementable action items towards sustaining CAT bond supporting CI markets in the long run. The main purpose of the action items being to (a) significantly reduce the CI supply-demand gap and (b) the increased purchase of standalone cyber insurance policies. The action items are targeted at cyber risk modelers, CAT bond investors, regulators, and bond-selling (re)insurers.

Strengthen the Data Science of Categorizing Cyber Incidents - A key stakeholder in the CAT bond driven CI market is the cyber risk modeling enterprise. The risk modeling enterprise in partnership with enterprise and CI firms should should use modern AI/ML technologies/ops (e.g., gradient boosted models, generalized linear models) over claims data, policy records over firmographic data, technographic data, and security ratings to categorize cyber incident types based on the extent to which frequency-severity data on such incidents is available and the degree of adverse impact spillover the incidents have across geographies and industries. This categorisation will result in the development of case-specific cyber risk quantification models, which are fundamental prerequisites to achieving successful ILS-driven CI markets. After all, no one size fits all! A model suited for large data availability cannot generate effective accuracy when it is applied to small data. While high/medium frequency cyber incidents (most data breaches, malware and DoS attacks) have lower spillover effects across geographies and industries on average, low frequency cyber-incidents usually have large spillover effects (e.g., AWS breakdown or a power grid breakdown for hours will affect all business sectors in a locality).

Ensure Data Science Driven Investor Sustainability - An investor will only stay in the market if the feasible values of CAT bond attributes make it economically viable for the investor to sustain itself in the market over time. At the same time, the attributes should also be viable for the (re)insurers to ensure 'harmony' (market equilibrium) between the supply and demand stakeholders. Contracts covering frequent cyber incidents with high availability of breach statistics across industries should usually mature in 1-2 years). The rationale is that the demand stakeholder side, i.e., the capital injectors, takes upon low spillover risk on high-frequency, low-impact cyber incidents for which considerable historical data is available for assessing cyber risk. Hence, investors expect to be paid low recurring interest by suppliers for a shorter time as they do not bear high risk.

Moreover, scenarios of high availability of breach statistics across industries suffer less from the problem of information asymmetry. This is the problem where insurers and capital investors do not have enough information on the cyber posture profile of cyber insured enterprises, which is a primary contributor to spillover effects. It is recommended that CAT bond contracts to manage such a class of cyber-incidents have a low multiplying risk premium factor, with indemnity triggers as the appropriate form of capital forego triggers. A significant quantity of breach statistics alongside insurance audits and Software Bills of Materials (SBOMs) helps infer the cyber-posture profile of enterprises. Industry partnerships (such as the recent one in 2024 between *Mosaic Insurance, Howden, Chubb, Liberty Specialty Markets*, and SAFE) to use modern AI/ML ops as an integral toolbox to invasive cyber posture estimation are the need of the hour. James Tuplin, Head of International Cyber, *Mosaic Insurance*, said: *"We believe inside-out scans powered by SAFE's software are the future. They're the best way to obtain direct, accurate information around*

an insured's cyber security posture, and offer far more insightful information, obtained more quickly and efficiently, than the standard application form process."

Contracts covering low-frequency, high-impact incidents with virtually no data availability should mature much later (a maximum of 10 years) and pay high interest rates to investors to prevent the latter from bearing the catastrophic risk of principal default. In such scenarios, the demand stakeholder side, i.e., the capital injectors, bears upon themselves a higher spillover risk on rare high-impact cyber incidents for which less historical data is available for assessing cyber risk. Hence, investors expect to be paid recurring (and higher) interest for a longer time by re-insurers for such incidents compared to frequent cyber incidents for which sufficient historical data is available.

Ensure Cyber (Re) Insurers Sustain in a CAT Bond Market - In principle, insurers will only participate in the CAT bond driven markets sustainably if the cost incurred to transfer cyber risk through CAT bonds is less than that incurred by retaining cyber risk in the form of the cost of equity (CoE). Currently, an insurance company's CoE is hardly impacted by cyber risk in its portfolio, as the latter reflects a paltry one percent of the total risk underwritten. Consequently, insurers usually pay recurring premiums to capital investors that are multiple times a fair premium amount so that the latter can hedge against extreme adverse impacts of (cyber) CAT event spillovers. As long as this multiplier is below a certain threshold, there will be a sustainable ILS-driven market between (re)insurers and capital investors. This situation is achievable only if there is (a) a considerable (if not significant) AI/ML ops catalyzed frequency-severity statistical data availability on cyber incidents to cyber risk modelers and (b) sufficient and AI/ML ops driven quality enterprise cyber-posture information shared (e.g., SBOMs) in public/private partnerships (on similar lines as the Howden, Liberty Speciality Markets, Chubb, SAFE, and Mosaic partnership). Regulators will play a key role in ensuring conditions (a) and (b). Alternatively, in the futuristic scenario when cyber risk will significantly reflect in an insurance company's portfolio, the CoE will be reduced via insurer diversification and ensuring actions (a) and (b). This will promote sustainable CAT bond driven CI markets.

7 SUMMARY

In this paper, we proposed the use of catastrophic (CAT) bonds (an example ILS product) as a radical residual cyber risk management methodology to boost much needed capital injection in the cyber (re)insurance business. We laid out a formal model of CAT bond markets and proposed conditions under which cyber insurers would find it economically sustainable to (a) only invest in retaining cyber risk of their enterprise clients, (b) transfer their risk to reinsurance companies, or (c) transfer their risk using a combination of reinsurance and CAT bonds. We proposed implementable action items for stakeholders of such markets to realize in practice the model results in theory that promote sustainable capital injection into CI markets.

REFERENCES

Braun, A. 2016. "Pricing in the Primary Market for CAT Bonds: New Empirical Evidence". *Journal of Risk and Insurance* 83(4):811–847.

Cummins, J. D. and P. Trainar. 2009. "Securitization, Insurance, and Reinsurance". *Journal of Risk and Insurance* 76(3):463–492.

Dambra, S., L. Bilge, and D. Balzarotti. 2020. "SoK: Cyber Insurance–Technical Challenges and a System Security Roadmap". In *2020 IEEE Symposium on Security and Privacy (SP)*, 1367–1383. IEEE.

Hofmann, A. 2007. "Internalizing Externalities of Loss Prevention through Insurance Monopoly: An Analysis of Interdependent Risks". *The Geneva Risk and Insurance Review* 32:91–111.

Khalili, M. M., P. Naghizadeh, and M. Liu. 2018. "Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence". *IEEE Transactions on Information Forensics and Security* 13(9):2226–2239.

Lelarge, M. and J. Bolot. 2009. "Economic Incentives to Increase Security in the Internet: The Case for Insurance". In *IEEE INFOCOM 2009*, 1494–1502. IEEE.

Marotta, A., F. Martinelli, S. Nanni, A. Orlando and A. Yautsiukhin. 2017. "Cyber-Insurance Survey". *Computer Science Review* 24:35–61.

Naghizadeh, P. and M. Liu. 2014, June 23-24. "Voluntary Participation in Cyber-Insurance Markets". In *Workshop on the Economics of Information Security (WEIS)*, 23–24. State College, PA, USA.

Pal, R., K. Duan, and R. Sequeira. 2025. "A Theory to Estimate, Bound, and Manage Systemic Cyber Risk". In *39th ACM SIGSIM Conference on Principles of Advanced Discrete Simulation*, 70–80.

Pal, R., K. Duan, R. Sequeira, and M. Siegel. 2024. "Is Systemic Cyber Risk Management for Enterprises Sustainable?". In *2024 Winter Simulation Conference (WSC)*, 572–583 https://doi.org/10.1109/WSC63780.2024.10838727.

Pal, R. and L. Golubchik. 2010. "Analyzing Self-Defense Investments in Internet Security under Cyber-Insurance Coverage". In *IEEE 30th International Conference on Distributed Computing Systems*, 339–347. Genoa, Italy: IEEE.

Pal, R., L. Golubchik, and K. Psounis. 2011. "Aegis A Novel Cyber-Insurance Model". In *Decision and Game Theory for Security*, edited by J. S. Baras, J. Katz, and E. Altman, 131–150. Berlin, Heidelberg: Springer Berlin Heidelberg.

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2014, April 27-May 2. "Will Cyber-Insurance Improve Network Security? A Market Analysis". In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, 235–243. Toronto, Canada.

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2017. "Security Pricing as Enabler of Cyber-insurance a First Look at Differentiated Pricing Markets". *IEEE Transactions on Dependable and Secure Computing* 16(2):358–372.

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2018. "Improving Cyber-Security via Profitable Insurance Markets". *ACM SIGMETRICS Performance Evaluation Review* 45(4):7–15.

Pal, R., Z. Huang, S. Lototsky, X. Yin, M. Liu, J. Crowcroft *et al*. 2021. "Will Catastrophic Cyber-Risk Aggregation Thrive in the IoT Age? A Cautionary Economics Tale for (Re-) Insurers and Likes". *ACM Transactions on Management Information Systems (TMIS)* 12(2):1–36.

Pal, R., Z. Huang, X. Yin, M. Liu, S. Lototsky and J. Crowcroft. 2020. "Sustainable Catastrophic Cyber-Risk Management in IoT Societies". In *2020 Winter Simulation Conference (WSC)*, 3105–3116 https://doi.org/10.1109/WSC48552.2020.9384051.

Pal, R., Z. Huang, X. Yin, S. Lototsky, S. De, S. Tarkoma *et al*. 2020. "Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re) Insurers and Likes". *IEEE Internet of Things Journal* 8(9):7360–7371.

Pal, R., P. Liu, T. Lu, and E. Hua. 2023. "How Hard is Cyber-Risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs". *ACM Transactions on Cyber-Physical Systems (TCPS)* 6(4):1–31.

Pal, R., T. Lu, P. Liu, and X. Yin. 2021. "Cyber (Re-) Insurance Policy Writing is NP-Hard in IoT Societies". In *2021 Winter Simulation Conference (WSC)*, 1–12 https://doi.org/10.1109/WSC52266.2021.9715524.

Pal, R., S. Madnick, and M. Siegel. 2023. "Trading in Catastrophe Bonds Can Boost Security Improving Cyber (Re-)Insurance Markets". In *Proceedings of Americas Conference on Information Systems (AMCIS)*, 1–10.

Pal, R. and B. Nag. 2024. "A Mathematical Theory to Price Cyber-CAT Bonds to Boost IT/OT Security". In *2024 Winter Simulation Conference (WSC)*, 648–659 https://doi.org/https://dl.acm.org/doi/10.5555/3643142.3643196.

Pal, R., K. Psounis, J. Crowcroft, P. Hui, S. Tarkoma, A. Kumar *et al*. 2020. "When are Cyber Blackouts in Modern Service Networks Likely? A Network Oblivious Theory on Cyber (Re) Insurance Feasibility". *ACM Transactions on Management Information Systems (TMIS)* 11(2):1–38.

Pal, R., R. Sequeira, and S. Zeijlemaker. 2024. "How Hard is it to Estimate Systemic Enterprise Cyber-Risk?". In *2024 Winter Simulation Conference (WSC)*, 560–571 https://doi.org/10.1109/WSC63780.2024.10838964.

Pfleeger, S. and R. Cunningham. 2010. "Why Measuring Security is Hard". *IEEE Security & Privacy* 8(4):46–54.

Shetty, N., G. Schwartz, M. Felegyhazi, and J. Walrand. 2010. "Competitive Cyber-Insurance and Internet Security". In *Economics of Information Security and Privacy*, edited by T. Moore, D. Pym, and C. Ioannidis, 229–247. Boston, MA: Springer US.

Yang, Z. and J. C. S. Lui. 2014. "Security Adoption and Influence of Cyber-Insurance Markets in Heterogenous Networks". *Performance Evaluation* 74:1–17.

AUTHOR BIOGRAPHIES

RANJAN PAL is a Research Scientist with the MIT Sloan School of Management, and an invited working group member of the World Economic Forum. His primary research interests lie in cyber risk and resilience management. He serves as an Associate Editor of the ACM Transactions on MIS, and is on the Technical Program Committees of ACM SIGSIM PADS and the Winter Simulation Conference. His email address is ranjanp@mit.edu.

BODHIBRATA NAG is a Professor with the Operations Management group at the Indian Institute of Management Calcutta India. His primary research interests include supply chain management and cybersecurity. His email is bnag@iimcal.ac.in.

SANDER ZEIJLEMAKER is a Research Affiliate with the MIT Sloan School of Management, and an agenda contributor to the World Economic Forum. His primary research interest lies in developing cyber risk governance solutions based upon system dynamics. His email is szeijl@mit.edu.

MICHAEL SIEGEL is a Principal Research Scientist with the MIT Sloan School of Management, and a co-director of MIT CAMS. His primary research interest lies in cybersecurity management of information systems. His email is msiegel@mit.edu.