Proceedings of the 2023 Winter Simulation Conference
C. G. Corlu, S. R. Hunter, H. Lam, B. S. Onggo, J. Shortle, and B. Biller, eds.

A MATHEMATICAL THEORY TO PRICE CYBER-CAT BONDS BOOSTING IT/OT SECURITY

Ranjan Pal
Sloan School of Management
Massachusetts Institute of Technology
E94, 245 First Street
Cambridge, MA 02142, USA

Bodhibrata Nag
Operations Management
Indian Institute of Management Calcutta
Diamond Harbor Road
Joka, West Bengal 700104, INDIA

ABSTRACT

The density of enterprise cyber (re-)insurance markets to manage (aggregate) enterprise cyber-risk has been low enough to realize their potential to significantly improve cyber-security and consequently the cyber-reliability of (ICS) enterprise ecosystems. In this paper, we propose the use of catastrophic (CAT) bonds as a radical and alternative residual cyber-risk management methodology to alleviate the big supply-demand gap in the current cyber (re-)insurance industry, by boosting capital injection in the latter industry. Two important follow up questions arise: (i) when is it feasible for cyber (re-)insurers to invest in CAT bonds? and (ii) how can we price cyber-CAT bonds conditioned on the feasibility condition(s)? We focus on answering the second question pivoted upon an existential answer to the first. We propose a novel practically motivated information asymmetry (IA) driven cyber-CAT bond pricing model, built upon theories of financial stochastic processes and Monte Carlo simulations, in realistic arbitraged incomplete markets.

1 INTRODUCTION

We live in the age of the industrial Internet-of-Things (IIoT) that is increasingly driving enterprises in (critical) service sectors such as water, telecom, power, finance, retail, energy, and transportation, among many others. These enterprises are individually shaped mostly by industrial control systems (ICSs) that use IoT technology to enhance the performance of industrial/enterprise operational processes via the use of smart devices and real-time analytics, and can be controlled, monitored, and managed over the Internet. According to corporate survey leader *Mordor Intelligence*, the global ICS market was worth approximately USD 108.68 billion in 2020 and is projected to reach USD 170.12 billion at an annual growth rate of 8.01% over the period 2021-2026, with smart cities around the globe likely to see the most rapid growth in ICSs.

Subsequently, the business continuity (BC) of each ICS controlled enterprise in any of these sectors today is a function of the reliability and resilience properties of its operational technology (OT) and/or IT subsystems spanned by IIoT. Here, 'resilience' is *the ability of enterprise processes to recover from, or more successfully absorb and adapt to adverse external and internal shocks (including cyber)* [mentioned in (Cutter et al. 2013) but is a standard in the research community] by providing a minimum acceptable level of business functionality performance. More importantly, these properties are further reliant on complex service inter-dependencies between ICSs controlled enterprises from various diverse sectors such as water, telecom, energy, power, transportation, manufacturing, retail, among many others. Amidst a traditionally weakly secure IIoT terrain, it is evident then that ICSs being left vulnerable to attack, can open the door to serious and worst case catastrophic events (e.g., *Stuxnet, Triton, NotPetya, Colonial Pipeline, Aurora*) resulting in rippling adverse economic, societal, and physical consequences faced by various stakeholders part of the ecosystem of inter-dependent enterprises. The scarily important lesson from past (ICS) cyber-incidents is not so much what happened as to what did not happen. ICS hackers did not push their limits by not poisoning water supplies, not melting down nuclear power plants, and not bringing down the power grid of an entire city – this, despite them successfully compromising critical infrastructure facilities. An important question that begs itself at this stage is: *why is it the case that the IIoT terrain is weakly secure?*

979-8-3503-6966-3/23/$31.00 ©2023 IEEE

1.1 The Inevitability of 'Below Par' IT/OT Security

It is not the case that IIoT security technology cannot be beefed up compared to current standards. Just that, the systems spanned by IIoTs will most likely have 'below par' security inevitably. *When compared to general IT systems, IT/OT driven ICS security is relatively more challenging – despite ICSs having a smaller functionality set and possibly smaller cyber-attack surfaces spanned by small sensor devices.* Why is this so? *To start with*, IIoT devices in ICSs deploy proprietary and legacy software and hardware interfaces that are often plagued with outdated vulnerabilities and/or misconfigured. As a result, in a large intra-organizational sensor network, ICS cyber-defenders usually do not have complete knowledge of which interfaces are running vulnerable software or are misconfigured. *Second*, ICS components (especially the field devices in Level 1 based on the standard Purdue ICS model) are often un-encrypted and/or unpatched, which puts them at risk of successful brute force password breaking events. In addition, patches for some firmware based on old OSs (e.g., Windows XP/NT) might not even be available. *Third*, critical ICSs are quite sensitive to downtime with respect to business continuity (QoS). Hence, the applicability of software patches requiring periodic system reboots can often be a hindrance to consumer QoS (as they need testing and approval prior to deployment). Moreover, these reboots results in loss of ICS (sub)system view that invites further system attacks during inter-booting time. *Finally*, it has been stated and proved by Cunningham et.al.,(Pfleeger and Cunningham 2010) and Pal et.al., (Pal et al. 2021; Pal et al. 2022) respectively (see details in Section 2), that the problem of discovering all possible cyber-vulnerable points in OT and IT systems is a Herculean task to accomplish computationally.

1.2 Enter Cyber-Insurance for ICSs

The above-mentioned challenges combined with the fact that (a) security technology is not perfect and (b) (behavioral) economic factors prevent perfectly rational actions taken by stakeholders (e.g., security product vendors, ICS employees, C-suites, regulators) in favor of optimized cyber-security, imply that, at best, ICS management can mitigate cyber-risk and consequently improve cyber-reliability but will not be able to eliminate cyber-risk. This is made evident by market statistics that showcase an approximately 18 billion USD current global ICS security market growing annually at around 6.6%, when the ICS cyber-loss valuation is at least 10-fold. As a result, the management of industrial control systems *(and broader IT systems in general)* in the last decade have resorted to cyber (re-)insurance as a risk management tool to alleviate residual cyber-risk and improve cyber-reliability – a practice that is a de-facto standard for non-cyber residual risk domains. For the general reader in the context of ICSs, residual cyber-risk is that portion of a post-incident cyber-risk that the client ICS cannot manage through traditional risk management tools such as vendor products (e.g., anti-virus, firewalls) 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*. However, in principle, cyber (re-)insurance solutions bring with them an added advantage of improving cyber-security provided there are enough buyers (Anderson and Moore 2009; Lelarge and Bolot 2009; Bolot and Lelarge 2008; Pal et al. 2014; Pal and Golubchik 2010; Pal et al. 2011; Pal et al. 2018a; Shetty et al. 2010a; Yang and Lui 2014; Biener et al. 2015; Romanosky et al. 2019). The rationale behind this is the fact that cyber (re-)insurance buyer premiums are a function of ICS cyber-postures – better postures resulting in lower premiums that flow from ICS to insurers and re-insurers, and vice-versa. It is then evident that a significant industrial population investing in cyber-solutions and aiming to pay as low premiums as possible will improve the security and resilience of the cyber-space spanned by them (Kesan et al. 2005; Odlyzko 2003).

1.3 A Weak/Sparse Cyber (Re-)Insurance Market

However, surprisingly enough, the current IT cyber-insurance market in practice (leave alone cyber-insurance specific to IT-OT converged ICSs) is severely sparse, i.e., low premium influx, when compared to their security and corporate welfare improving need in society. In other words, there is a market failure on the

supply and demand of cyber-insurance contracts. More specifically, the current annual cyber-insurance market (includes insurance for ICSs) is worth a maximum of 20 billion USD globally, when the annual cyber-loss valuation is greater than a trillion USD in a trillion dollar capacity, leaving the digital society bearing the adverse impact of billions of dollars of un-managed cyber-risk every year. The primary reasons for this trend being (a) high information asymmetry (IA) between the insurer and the insured driven by inter-dependent and correlated cyber-risk among businesses, (b) aggregate supply chain cyber-risk, and (c) IA-driven unattractive premium/deductible charged to insured businesses. This lack of much needed capital results in large market inefficiencies in cyber-risk diversification markets that does not allow the huge potential of cyber-insurance products to significantly boost security of enterprises and their ecosystems (Wolff 2022). These viewpoints have also been recently echoed by Zurich chief Mario Greco who feels that enterprise cyber-attacks (especially those on critical infrastructure) might become uninsurable with growing business disruptions due to them. One could argue here that cyber-insurers could hedge their own risk with re-insurers in scenarios of inter-dependent, correlated, and aggregated cyber-risk (e.g., as those arising from ICSs). Profit minded and risk averse cyber-insurance companies indeed have often disproportionately relied on cyber re-insurance businesses (providing insurance for cyber-insurance firms) for support to cover client cyber-losses in large and growing service dependent supply chain network settings carved out by ICSs. To this end, it is very popular among cyber-insurance firms to shift approximately more than 50% of cyber-insurance premiums to the re-insurance market (and hence not being completely liable for their client-facing risks) of not many (likely less than 10) suppliers. Hence, with only a small set of cyber re-insurers in the risk management market, it is not surprising that near-term supply of (ICS) cyber-insurance solutions will fall far below the demand. *Subsequently, without any radical change in how cyber (re-)insurance markets are 'operated', the vision of using cyber (re-)insurance products to significantly improve ICS (and OT/IT) security and reliability will likely fall apart in digital societies.*

1.4 Towards a Radical Residual Risk Management and Reliability Boosting Methodology for ICSs

Looking to a future and densely connected ICS ecosystem, cyber-insurance markets capable of controlling the ICS cyber-posture in favor of a secure cyber-space carved out by ICSs need to scale big. In this paper we argue in favor of a radical methodology to transfer residual first and third party cyber-risk faced by ICSs (extends to general OT and IT industries) specific to interdependent service supply chain environments, using catastrophe bonds. This especially so with *Beazley* recently announcing the first cyber-CAT bond in January 2023 with the goal to create a dynamic market boosting cyber (re-)insurance services. The goal of the methodology is to simply scale/densify cyber (re-)insurance markets to improve cyber-security and reliability (in ICSs) for the social good by injecting additional capital currently lacking in such markets - such a capital sourcing from risk-loving hedge funds who trade (re-)insurance cyber-risk in a multi-trillion dollar financial market. *We envision that the practice of an increasing number of risk-averse cyber re-insurance companies selling catastrophe bonds to financial traders (e.g., by hedge fund companies) in the form of insurance-linked securities (ILSs) in the non-correlated multi-trillion (approximately 40 trillion USD currently) financial markets will significantly densify cyber re-insurance and cyber-insurance markets, and boost cyber-security in the (inter-networked) ICS space.* The basic working logic behind the use of ILSs is that the aggregate and correlated (supply chain) cyber-risk can be diversified among a significantly larger set of traders in an independent financial market when compared to a much smaller (akin to a *'drop in the ocean'*) set of re-insurers in a dependent insurance market. In this way financial traders (e.g., hedge funds) can take more risk through ILSs in the expectation of higher monetary returns.

1.5 Research Goal and Contributions

Our long-term **research goal** is to realize the vision of cyber-ILS markets through a practically motivated rigorous formulation of (a) the conditions under which a market for cyber-insurance linked securities (CILSs) can prosper, and (b) pricing constructs for such CILSs. *In this paper, we only focus on the pricing*

aspect of CILSs conditioned on the assumed existence of feasible conditions for prosperous CILS markets. Consequently, we propose the following **contributions**.

1. We introduce the concept of catastrophic (CAT) bonds as an example of cyber-insurance linked securities (CILSs) that can in principle significantly boost cyber-security in interdependent (supply chain) ICS environments in a radical fashion via boosted cyber (re-)insurance markets. To this end, we first provide an elaborate and intuitive explanation on why trading of CAT bonds (e.g., by hedge funds through entities such as Goldman Sachs) can be highly effective in adding substantial capital to boost less correlated (to financial stability) cyber re-insurance and cyber-insurance markets. We subsequently argue that a boosted capital injection is equivalent to denser residual cyber-risk management markets and improved cyber-security and reliability in the ICS space **(see Section 2)**.
2. We propose a stochastic jump-diffusion process based and practically motivated optimal CILS pricing mechanism for CAT bonds that accounts for the inevitable incompleteness of CILS markets and the obvious presence of financial arbitrage under IA - degree of lack of information on correlation between cyber-posture and financial stability. The necessity to consider a stochastic jump process (instead of a traditional stochastic process comprising i.i.d random variables) to price CAT bonds arises from the fact that the volatility (think of variance) in ICS cyber-risk impact over time might not be a constant over time in practice, and might exhibit sharp 'jumps' from any time instant. This is because major cyber-attacks are hardly periodic and so are their impacts. Hence, the volatility of CAT bond prices over time should subsequently exhibit similar jumps. We conduct analysis on a continuous process space for the purpose of mathematical tractability, and without loss of generality. Our proposed Monte Carlo pricing theory is in stark contrast to existing works in the finance literature on traditional ILS markets that ideally assume completeness and/or zero financial arbitrage - neither of which is true in practice. We show IA to be a main driver of price attractiveness to CILS traders **(see Section 3)**. This result corroborates and correlates with our hypothesis (verifying which is not within the scope of this paper) that if IA (w.r.t. the cyber (re-)insurers and their insureds) is high for cyber-CAT bond traders, investing in such cyber-risk hedging and reliability boosting services is not cost effective for cyber (re-)insurers. The converse result, boosting capital and cyber-security/reliability, holds if IA is low for cyber-CAT bond traders.

Research Novelty and Applicability - To the best of knowledge, this is the first paper putting forward the idea of using insurance-linked securities such as cyber-CAT bonds to inject much-needed capital to densify cyber-security and cyber-reliability improving cyber (re-)insurance markets.

2 HOW CAN ILS SOLUTIONS DENSIFY CYBER-INSURANCE MARKETS?

The overarching root issue with current cyber-insurance markets is the lack of enough capital with re-insurers and insurers for them to scale their businesses, and contributed by reasons mentioned in the previous section. This lack of much needed capital results in market inefficiencies in cyber-risk diversification markets. The big question at hand then becomes: is there a way to boost capital injection in such markets? *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 (cyber-)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 trading securities in non-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)

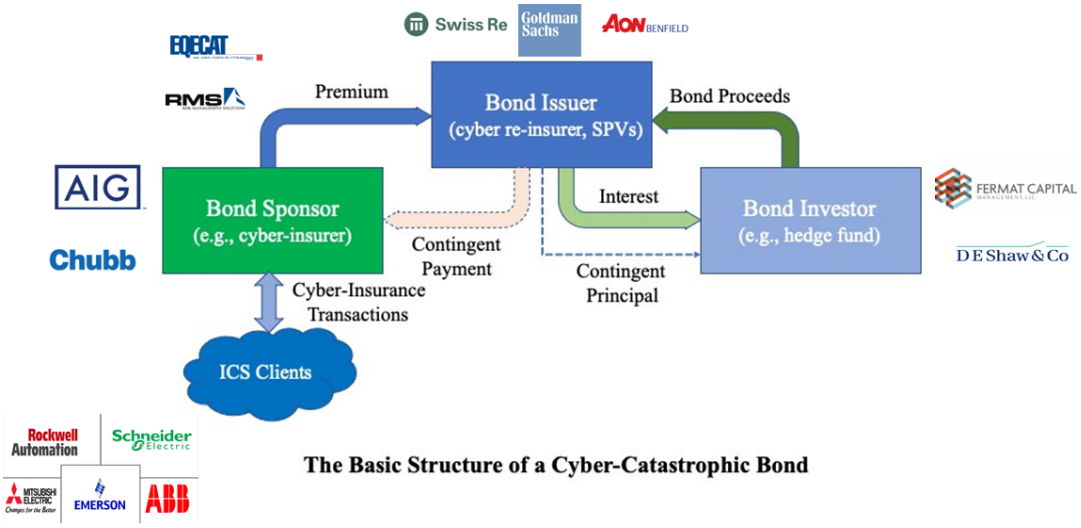

Figure 1: A structured illustration of a catastrophic (CAT) bond functionality with stakeholder examples

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 cyber-insurance markets – thereby also improving the ILS market in return. Since the early 1990s, ILS funds have provided retrocession (re-insurance for re-insurers) to the property-catastrophe re-insurance market for hurricanes and earthquakes when their capital is in short supply. ILS funds provide protection for rare events, and hence are able to generate (a) enough returns for their investors, and (b) much required capital for cyber (re-)insurers to manage (catastrophic) cyber-risks more effectively and improve system reliability. In the context of insuring ICS cyber-risks and especially in the age of rising ransomware demands, cyber-insurers can get enough capital injected into their business (through re-insurers) using ILSs to be able to rapidly proliferate markets with contracts that are not lemons. This, alongside the fact that ICS-operated smart cities around the globe are growing fast, will densify cyber (re-)insurance markets for the social good. Having discussed the logic of ILSs behind boosting cyber (re-)insurance capital, we now briefly touch upon (for the sake of completeness) 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). In the context of cyber-space, when a 'rare' catastrophe occurs (e.g., a critical ICS plant shuts down for days at a stretch) within a bond term (e.g., two years), the bond sponsor (the cyber-insurer paying premiums 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 re-insurance 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 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 functioning mechanism of financial CAT bonds is illustrated in Figure 1.

3 HOW SHOULD WE PRICE CYBER-CAT (IN CONTRAST TO NON-CYBER CAT) BONDS?

In this section, we address the problem of how CILSs should be priced for such newer cyber-risk environments (in contrast to traditional financial risk), under the assumption that necessary conditions for the existence of CILS markets have been satisfied (not the scope of this paper).

Two Primary Pricing Challenges - One should ensure that CILSs are priced within an environment of *incomplete financial markets*. Such markets are a reality and characterized by the fact that there will exist situations where underlyings (e.g., cyber-loss indices) will be non trade-able. This is in contrast to complete financial markets (in the *Arrow-Debreu* sense) where there is perfect information on trade-able asset/underlying (e.g., an accurate information on organizational cyber-posture that drives cyber-risk to be traded), an hence there is a price for every asset/underlying in every possible state of the world. *The first challenge we face in this paper in applying existing CILS pricing methodologies from the broader finance research literature due to their lack of modeling incomplete trading markets* (Nowak and Romaniuk 2013; Nowak and Romaniuk 2018). However, the dimension of cyber-risk hedging makes financial markets more incomplete than ever, and this needs to be accounted for. In addition, there is the inevitable presence of financial arbitrage in trading markets implying that CILS trading markets will usually mis-price trade-able assets/underlyings, before they eventually correct and the assets move back to statistically fair, i.e., expected, values. In practice, CAT bonds usually trade at significant margins above the expected loss covered by the hedge (Froot 2001). This is done by practitioners by setting arbitrage-dependent CILS prices to the expected value plus a function of the second moment of the loss distribution in order to take into account risk aversion; and with the corresponding probability of occurrence being obtained from a sample of historical observations. However, this practice is only valid in the context of large diversified portfolios of identical and independently distributed (i.i.d) risks (typical of the standard insurance industry) that follow the statistical Law of Large Numbers (LLN). It is evident that cyber-risks are not i.i.d, and *hence our second challenge stems from the inability to apply existing arbitrage-dependent CILS pricing methodologies in the traditional finance research literature to our pricing problem.*

Our Approach - We use the seminal methodology proposed in (Merton 1976) to form the base of our proposed CILS pricing approach. The basis of (Merton 1976) is a *jump-diffusion* (a stochastic process) model that allows us to capture abrupt jumps (catastrophe events being one of the causes) in the index of underlyings that trade in the financial market, and whose risk (of occurrence) can be diversified. Moreover, the methodology in (Merton 1976) can be easily extended to apply to incomplete market settings.

3.1 Pricing Model Setup

Formalizing a Cyber-CAT Bond Structure - We assume the cyber-CAT bond payoff structure to be binary. A CILS is akin to a corporate bond with cyber-insurance risk instead of default risk. The bondholder, i.e., a CILS trader such as a hedge fund, expects to lose interest or a fraction of the invested principal if a cyber-risk index (a proxy for cyber-posture of a portfolio of cyber-insured organizations), whose value at date t is denoted I_t, hits a pre-specified threshold K. In other words, conditioned that the cyber-risk index does not reach K during a risk-exposure period T, the bondholder is paid a face value F - else it receives F minus a write-down coefficient in percentage w. Let T' be the instant when the cyber-CAT bond expires, where T is assumed to be greater than T to account for possible lags in the cyber-risk index assessment at expiration of the CILS instrument.

Formalizing the Structures of Dynamic Bond Parameters - Let $(\Omega, \mathscr{I}, P)$ be a standard probability space. Here, Ω represents the set of states of the world - consisting of all possible cyber-loss states for a cyber re-insurer post a cyber-breach incident, $\mathscr{I}$ is a σ-algebra of subsets of Ω (the set of all possible events induced by the incident) and P is a probability measure on I. Processes are defined on this probability space and on a trading horizon $[0, T']$. We consider two standard Brownian motion stochastic processes: $\{W_t : 0 \leq t \leq T'\}$ and $W_{2t} : 0 \leq t \leq T'$, and a Poisson process, $\{N_t : 0 \leq t \leq T\}$, with an intensity parameter λ_p. Furthermore, let $\{U_j : j \geq 1\}$ be a sequence of i.i.d. random variables with values in $]1; +\infty[$; U_j occurs at time τ_j defined by (N_t), i.e., $\tau_j = \inf\{0 \leq t \leq T', N_t = j\}$. We assume that the σ-fields generated by the stochastic processes $(W_t), (W_{2t}), (N_t)$, and (U_j) are independent. This assumption is justified by the fact that *these four sources of randomness in a CILS market account for non-catastrophic cyber-risk events, the time-dependent uncertainty of non-spot interest rates (as a result of pricing under arbitrage), the occurrences of cyber-catastrophes, and the cyber-loss impact (as a faced by a cyber re-insurer) of*

cyber-catastrophes, respectively. All these four sources are dependent on (i) the information asymmetry (IA) faced by cyber (re-)insurers on the (aggregate) cyber-loss values incurred by their clients, and (ii) the maximum tolerable IA. In modeling terms, (i) and (ii) would represent statistical noise (e.g., Gaussian noise) over actual cyber-loss amounts and captured via random variables. For all t in $[0,T']$, let F_t be the σ-field generated by the random variables W_s, W_{2s}, N_s for $s \leq t$, and $U_j \mathbf{1}_{j \leq N_t}$ for $j \geq 1$. Then the mathematical filtration $\{F_t : 0 \leq t \leq T'\}$ represents the (increasingly-enriching) information flow regarding the dynamics of the cyber-risk world reaching CILS market stakeholders over time. (F_t) is augmented to encompass all P-null events, each with probability measure zero.

A Formal CILS Trading Market - We model a financial trading market as that without friction - having no transaction costs (without loss of generality), and a place where CILS trading can take place continuously over time. The decision to omit transaction costs is taken to achieve analytical simplicity, without missing out on any relevant insights that we wish to achieve from our proposed theory. A continuous trading activity is modeled, only for the purpose to fit a continuous theory that is more general than a discrete trading theory (rather than the other way around). To this end, we assume that the cyber-risk free (from here on, just risk-free, unless otherwise specified) interest rates obey a mean-reverting process. In technical terms, a risk-free interest rate on any investment is a purely theoretical concept, given that most investments in practice accompany risk. However, although it is possible for cyber re-insurers (or special purpose vehicles (SPVs) associated with the latter to design CILS contracts) to default on its securities, the likelihood of this event is quite low (though there is a high probability of large, if-not default-type, cyber-losses from correlated and interdependent cyber-risk from ICS cyber-breaches). In the context of cyber-risk, this likelihood value is perceived to be low enough (by cyber (re-)insurers) currently, and hence we work with "cyber-risk free" cyber-CAT bonds. However, we do emphasize that our proposed theory can be easily extended to the case of risky interest rates. Mathematically, the risk-free spot interest rate r (captured as distribution to implement financial arbitrage) follows the dynamic process (expressed as a stochastic differential equation), under the historically and empirically obtained probability measure P:

$$dr(t) = a(b - r(t))dt + \sigma_r dW_{2t},$$

where a, b, and σ_r (volatility of r) are constants. A mean-reverting process is characteristic of events that are cyclical in nature. A cyber-catastrophe is one of these events. Note a stochastic differential equation (SDE) modeling time-varying, and most importantly abruptly-jumping, cyber-risk free interest rates captures their precise uncertainty due to perceived-varying cyber-posture effects over time. The CILS traders are assumed to invest in zero-coupon bonds sold by a cyber (re-)insurer or a special purpose vehicle (SPV) associated with the cyber (re-)insurer, and subsequently take higher risks because they do not get paid periodic interest, but profit from buying the bond at a value far lesser than the face value of the bond, and get paid at full maturity with interest. This assumption is practical in the sense that CILS traders are investing in the long-term to generate wealth from catastrophic cyber-incidents - for such long-term scenarios zero-coupon bonds are one standard (Vasicek 1977). We also assume that the cyber-risk index (a proxy to the cyber-posture of a portfolio of organizations whose cyber-insurance is handled by a cyber re-insurer), that acts as a pivot using which CILS markets are traded in financial markets, is driven by a Poisson jump-diffusion process. A Poisson process is a natural choice due to the counting nature of cyber-catastrophe incidents, given that the Poisson process is a counting stochastic process. This process, denoted by $(I_t)_{t \geq 0}$, is right-continuous and satisfies the following:

$$\frac{dI_t}{I_{t^-}} = \mu(t)dt + \sigma(t)dW_t + J_t dN_t.$$

This equation consists of three components: the change in the expected instantaneous cyber-risk index when there is no occurrence of cyber-catastrophe, the unanticipated instantaneous index change, and the instantaneous change in the cyber-risk index when a cyber-catastrophe occurs. I_t^- stands for the cyber-risk

index value at an incremental time instant prior to t;$\mu(\cdot)$is the drift parameter pertaining to the cyber-risk index, and can be stochastic; $\sigma(\cdot)$ is a deterministic volatility parameter of the geometric Brownian component of the jump-diffusion process; (N_t) is a Poisson process accounting for the expected number of jumps per time unit; and (J_t) depicts the stochastic size of the jumps, and is defined by the following relation:

$$J_t = \sum_{n=1,+\infty} U_n \mathbf{1}_{[\tau_{n-1},\tau_n]}(t),$$

where (U_j) and (τ_j) are defined as mentioned above, i.e., at time τ_j, the jump of I_t is given by

$$\triangle I_{\tau_j} = I_{\tau_j} - I_{\tau_j^-} = I_{\tau_j^-} \times U_j, \text{ or } I_{\tau_j} = I_{\tau_j^-}(1+U_j).$$

$J_t dN_t$ is then a compound Poisson process, with $(1+U_j)$'s being log-normally i.i.d (with shifted support). The assumption of this log-normality is not restrictive, as many distributions can be derived through it.

3.2 Results Derived Through Pricing Model Analysis

In this section, we state our main results as an outcome of analyzing our CILS pricing model based upon (Vaugirard 2003). Our first pricing result most importantly guarantees the existence of an arbitrage-accommodating price of a cyber-CAT bond in incomplete CILS trading markets, and generalizes its price.

Theorem 1 *There exists an arbitrage-accommodated price of a cyber-CAT bond in incomplete CILS trading markets. Let (a) $CCB(t)$ be such a price of the cyber-CAT bond issued to a CILS trader at time t, (b) $T_{1,K}$ the first passage (FP) time of 1 through K, and (c) cash payments are transferred to the CILS trader at a maturity date T'. Then,*

$$CCB(t) = FP(t,T')\left\{1 - wE^Q\left(\frac{\mathbf{1}_{T_{1,K}\leq T}}{F_t}\right)\right\},$$

where Q is the unique restriction to the σ-field generated by W and W_2 of any equivalent martingale measure, and F_t is the face value of the cyber-CAT bond at any given time instant. $D(t,T') = exp(-\int_{t,T} r(u)du)$ is the stochastic discount factor, and the the dynamics of I and r under Q is given by

$$\frac{dI_t}{I_{t^-}} = (\mu(t) - \lambda(t)\sigma(t))dt + \sigma(t)dW_t' + J_t dN_t$$

and

$$dr(t) = a(b^* - r(t))dt + \sigma_r dW_{2t}'.$$

Here, $\lambda()$ is the market price of catastrophic cyber-risk, W and W_2 are the Q-standard Brownian motion that maps to the P-standard Brownian motion W and W_2 (obtained via the celebrated Girsanov Theorem (Liptser and Shiriaev 1977)). Moroever, we have

$$P(t,T') = \exp[-(T'-t)R(T'-t, r(t))]$$

with,

$$R(\theta, r) = R_\infty - \left[\frac{1}{a\theta}\right]\left\{(R_\infty - r)(1-e^{-a\theta}) - \left[\frac{\sigma_r^2}{4a^2}\right](1-e^{-a\theta})^2\right\};$$

$$R_\infty = b^* - \left[\frac{\sigma_r^2}{2a^2}\right].$$

Practical Implications of the Theorem - The theorem most importantly proves the existence of an arbitrage-dependent price of cyber-CAT bonds in an incomplete CILS trading market equilibrium. It also provides a closed form expression to the cyber-CAT bond price in relation to the degree of information asymmetry

CILS traders are exposed to. With increasing (aggregate of first and third party) cyber-risk faced by cyber (re-)insurers, the cyber-CAT bond price evidently decreases. In the face of high information asymmetry (IA) regarding the extent of cyber-risk cyber (re-)insurers are exposed to, high IA on organization cyber-posture will lead to lower $CCB(t)$ values when compared to that in low IA scenarios. Equivalently, high/low IA gaps are proportional to the distance between actual cyber-risk index level and the bond trigger level. In addition, if the variance of the cyber-risk index increases, the cyber-CAT bond price evidently decreases. Finally, the price of a cyber-CAT bond decreases with (a) an increased time to maturity - supplying more profit to the cyber-CAT bond holder, i.e., CILS traders, and (b) higher rate of the (compound) Poisson process. The primary reason for this trend being the increased time to and higher probability of witnessing a cyber-catastrophe event that is a result of (a) and (b). The theorem also provides insights into the yields obtained from the priced cyber-CAT bonds. The yield spread evidently increases with the length of time that organizational cyber-resources are exposed to cyber-risk, and is concave with respect to the time of bond maturity. We state our second CILS pricing result, motivated from the Monte Carlo theory in (Vaugirard 2003), of the closed form for cyber-CAT bond prices under specific catastrophe impact conditions.

Theorem 2 *Suppose that the cyber-risk index signal is such that it indicates (a) a cyber-catastrophe with a high adverse impact to the cyber (re-)insurer, and (b) a cyber-catastrophe with a medium-scale adverse impact to the cyber (re-)insurer, there exists an arbitrage-accommodated price of a cyber-CAT bond in incomplete CILS trading markets, for both (a) and (b). The closed form expressions for the price of a cyber-CAT bond in these cases are given by*

$$(i)CCB_{high} = Fe^{-rT}(1 - wE^{Q}(1_{T_{1,K\leq T}})),$$

with

$$E^{Q}(1_{T_{1,K\leq T}}) = e^{-\lambda T}\left\{N(d_1) + \left(\frac{I_0}{K}\right)^{1-\frac{\delta}{\sigma^2}} N(d_2)\right\} + (1 - e^{-\lambda_p T}),$$

where

$$d_1 = \frac{\ln(\frac{I_0}{K}) + (\delta - \frac{\sigma^2}{2})T}{\sigma T^{1/2}}, d_2 = \frac{\ln(\frac{I_0}{K}) - (\delta - \frac{\sigma^2}{2})T}{\sigma T^{1/2}}$$

with $\delta = \mu - \lambda\delta$.

$$(ii)CCB_{medium} = Fe^{-rT}(1 - wE^{Q}(1_{T_{1,K\leq T}})),$$

where $E^{Q}(1_{T_{1,K\leq T}})$ *can be obtained via iterations of a Monte Carlo algorithmic setup as*

$$I_{n+1} = \{[1 + (\mu(\frac{T_n}{N}) - \lambda(\frac{T_n}{n})\sigma(\frac{T_n}{n}))]\Delta t + \sigma(\frac{T_n}{n})g(0,1)\sqrt{\Delta t} + \sum_{j=1,N(\lambda_p\Delta t)} [\exp(g_j(kv,\delta)) - 1]\},$$

and

$$r_{n+1} = a(b^*)\Delta t + (1 - a\Delta t)r_n + \sigma_r g_2(0,1)\sqrt{\Delta t}.$$

Here, N denotes the step count, $\Delta = \frac{T}{N}$, $kv = \ln(1 + E(U_1))$, *and* $\delta^2 = variance(\ln(1+U))$, *and where* $g(0,1)$, $g_2(0,1)$, *and* $g_j(kv,\delta)$ *are sampled from independent normal distributions,* $\mathcal{N}(0,1)$ *and* $\mathcal{N}(kv,\delta)$ *respectively.* $N(\lambda p\Delta t)$ *is induced using a Monte Carlo simulation of a Poisson r.v., N, of intensity* θ, *through the following relation,*

$$N_\theta = \sum_{n\geq 1} n 1_{\{UF_1 UF_2 \ldots UF_n \leq e^{-\theta} \leq UF_1 UF_2 \ldots UF_n\}},$$

where $(UF_i)_{i\geq 1}$ *are independently and uniformly distributed on [0,1]. An incremental (over I from 1 to K) test procedure is then initiated to see if the cyber-risk index hits a barrier during the a cyber-risk exposure period, and* $E^{Q}(1_{T_{I,K\leq T}})$ *is subsequently obtained by averaging over the number of trajectories.*

Practical Implications of the Theorem - This theorem most importantly proves the existence of an arbitrage-dependent price of cyber-CAT bonds in an incomplete CILS trading market equilibrium - this time, specifically for scenarios pertaining to different degrees of cyber-CAT impact on occurrence. It also provides a closed form expression to the cyber-CAT bond price in relation to the degree of information asymmetry CILS traders are exposed to. The trends for the variations in cyber-CAT bond prices with respect to (a) cyber-risk index faced by cyber (re-)insurers, (b) information asymmetry on organizational cyber-postures, (c) variance of cyber-risk, (d) time to bond maturity, and (e) parameters of a (compound) Poisson process, are the same as in Theorem 1, and for similar reasons.

4 RELATED WORK

In this section, we provide a brief overview of research related to our efforts. *To the best of our knowledge, there is no existing work that formally (or informally) studies pricing of cyber-catastrophic bonds as capital-injecting solutions to boost cyber (re-)insurance markets.* Here by the term 'market', we imply a (aggregate) cyber-risk hedging market through CILS products (e.g., CAT bonds) in the presence of information asymmetry (IA). *Hence, our efforts in this paper are completely new in that regard.* Nonetheless, we categorize related research in this section into two themes pertaining to residual cyber-risk management (RCRM) in organizations - the overarching topic of our research: (i) the success of cyber-insurance markets, and (ii) the success of cyber re-insurance markets aggregating cyber-risk from IT/ICS enterprises.

4.1 On Success (Efficiency) of Cyber-Insurance Type RCRM Markets

Introductory foundational research works on cyber-insurance (Lelarge and Bolot 2009; Shetty et al. 2010b) have mathematically shown the existence of economically inefficient insurance markets. In (Pal and Golubchik 2010), the authors proposed a Coasian bargaining approach among cyber-insured network entities to achieve an efficient insurance market. Lelarge et al. in (Lelarge and Bolot 2009) recommended the use of fines and rebates on cyber-insurance contracts to make each user invest optimally in self-defense and achieve efficient cyber-insurance markets. In relative more recent works (Pal et al. 2011; Pal et al. 2014; Pal et al. 2018b; Khalili et al. 2018), the authors propose ways to form provably efficient monopolistic cyber-insurance markets by satisfying market stakeholders, including a risk-averse cyber-insurer, in environments of interdependent risk with partial IA. The authors in (Naghizadeh and Liu 2014; Pal et al. 2011) further state the importance of compulsory insurance for maximizing efficiency of primary cyber-insurance markets. As an orthogonal contribution to the above, the authors in (Pal et al. 2022) computationally justify the fact that optimal cyber-risk diversification task enroute to underwriting of cyber-insurance contracts for enterprises under informational asymmetry (IA) issues is computationally hard (that directly affects the success of cyber-insurance markets).

4.2 On the Efficiency of Re-insurance Type RCRM that Aggregates Cyber-Risk

Re-insurance type RCRM product businesses to manage catastrophic cyber-incidents in enterprises are in a similar boat as their traditional cyber-insurance counterparts when it comes to facing the brunt of IA between the supply and the demand sides. More so, because *the systemic nature of cyber and the potential for losses that transcend geography, industry, and class, is leading to the rapid demand for aggregate cyber-risk coverage on multiple service supply chain lines of service-networked businesses in IT/IoT driven societies.* There are quite a few instances in practice where individual cyber-risks (a candidate cyber-risk distribution on each of these lines) have shown heavy-tailed impact (Maillart and Sornette 2010; Wheatley et al. 2016). There are also studies establishing the dependence among cyber risks. Notable among them are (Herath and Herath 2011; Pal et al. 2019; Mukhopadhyay et al. 2013; Böhme and Kataria 2006; Peng et al. 2018; Wheatley et al. 2021). In all these statistics, IA has a crucial role to play in the sense that IA-mitigating policies and subsequent organizational liabilities in operation could in the first place prevent the cyber-risks becoming heavy-tailed. In a recent set of works (Pal et al. 2021; Pal et al. 2020; Pal et al.

2020), the authors develop the first formal analysis frameworks to decide the feasibility and sustainability of aggregating a set of (correlated) cyber-risks with heterogeneous tail properties, for a cyber-risk aggregating RCRM business. As a new result (in contrast to empirical ones), they formally prove that even i.i.d., heavy-tailed cyber-risks of certain types are not commercially suitable for aggregation by the RCRM firms - leave alone correlated ones. Hence, cyber re-insurance markets are also likely to be significantly inefficient. **Differences** - *Our research in this paper starts off with the motivation that the above ideas have still not mitigated enough the market in-efficiency of cyber (re-)insurance markets.* Recent market studies still suggest not enough capital being injected into current cyber (re-)insurance markets. To this end, our main focus in the paper (in contrast to above-mentioned existing works) is to first study the concept of alternative cyber-risk management solutions such as CILSs to mitigate residual market inefficiency and subsequently derive a pricing model for such solutions. In the CILS space, we are the first to derive pricing constructs.

5 SUMMARY

In this paper, we proposed the use of catastrophic (CAT) bonds as a radical residual cyber-risk management methodology to alleviate the big supply-demand gap in the current cyber (re-)insurance industry, by boosting capital injection in the latter industry. We proposed an optimal CILS pricing mechanism for CAT bonds that accounts for practical constraints such as an inevitable incompleteness of CILS markets and the obvious presence of financial arbitrage. Our pricing theory showcased that it is imperative to significantly mitigate cyber-risk related information asymmetry (much more than in traditional ILS markets) in IT/ICS-driven organizations to reap the cyber-security improving and (re-)insurance capital boosting benefits of CILSs.

REFERENCES

Anderson, R., and T. Moore. 2009. "Information Security: Where Computer Science, Economics and Psychology Meet". *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 367(1898):2717–2727.

Biener, C., M. Eling, and J. H. Wirfs. 2015. "Insurability of Cyber Risk: An Empirical Analysis". *The Geneva Papers on Risk and Insurance-Issues and Practice* 40(1):131–158.

Böhme, R., and G. Kataria. 2006. "Models and Measures for Correlation in Cyber-Insurance.". In *WEIS*.

Bolot, J.-C., and M. Lelarge. 2008. "A New Perspective on Internet Security using Insurance". In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, 1948–1956. IEEE.

Cutter, S. L., J. A. Ahearn, B. Amadei, P. Crawford, E. A. Eide, G. E. Galloway, M. F. Goodchild, H. C. Kunreuther, M. Li-Vollmer, M. Schoch-Spana et al. 2013. "Disaster Resilience: A National Imperative". *Environment: Science and Policy for Sustainable Development* 55(2):25–29.

Froot, K. A. 2001. "The Market for Catastrophe Risk: A Clinical Examination". *Journal of Financial Economics* 60(2-3):529–571.

Herath, H., and T. Herath. 2011. "Copula Based Actuarial Model for Pricing Cyber-insurance Policies". *Insurance Markets and Companies: Analyses and Actuarial Computations* 2(1):7–20.

Kesan, J., R. Majuca, and W. Yurcik. 2005. "Cyberinsurance as a Market-based Solution to the Problem of Cybersecurity: A Case Study". In *WEIS*.

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.

Liptser, R. S., and A. N. Shiriaev. 1977. *Statistics of Random Processes: General theory*, Volume 394. Springer.

Maillart, T., and D. Sornette. 2010. "Heavy-tailed Distribution of Cyber-risks". *The European Physical Journal B* 75(3):357–364.

Merton, R. C. 1976. "Option Pricing when Underlying Stock Returns are Discontinuous". *Journal of Financial Economics* 3(1-2):125–144.

Mukhopadhyay, A., S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan. 2013. "Cyber-risk Decision Models: To Insure IT or Not?". *Decision Support Systems* 56:11–26.

Naghizadeh, P., and M. Liu. 2014. "Voluntary Participation in Cyber-insurance Markets". In *Workshop on the Economics of Information Security (WEIS)*.

Nowak, P., and M. Romaniuk. 2013. "Pricing and Simulations of Catastrophe Bonds". *Insurance: Mathematics and Economics* 52(1):18–28.

Nowak, P., and M. Romaniuk. 2018. "Valuing Catastrophe Bonds Involving Correlation and CIR Interest Rate Model". *Computational and Applied Mathematics* 37(1):365–394.

Odlyzko, A. 2003. "Economics, Psychology, and Sociology of Security". In *Financial Cryptography*.

Pal, R., and L. Golubchik. 2010. "Analyzing Self-Defense Investments in Internet Security under Cyber-Insurance Coverage". In *Proceedings of 2010 IEEE 30th International Conference on Distributed Computing Systems*, 339–347. Los Alamitos, CA, USA: Institute of Electrical and Electronics Engineers, Inc.

Pal, R., L. Golubchik, and K. Psounis. 2011. "Aegis: A Novel Cyber-insurance Model". In *International Conference on Decision and Game Theory for Security*, 131–150. Springer.

Pal, R., L. Golubchik, K. Psounis, and T. Bandyopadhyay. 2019. "On Robust Estimates of Correlated Risk in Cyber-Insured IT Firms: A First Look at Optimal AI-Based Estimates under "Small" Data". *ACM Transactions on Management Information Systems (TMIS)* 10(3):1–18.

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2014. "Will Cyber-insurance Improve Network Security? A Market Analysis". In *INFOCOM, 2014 Proceedings IEEE*, 235–243. IEEE.

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

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2018b. "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, N. Sastry, S. De, and B. Nag. 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, S. Lototsky, S. De, S. Tarkoma, M. Liu, J. Crowcroft, and N. Sastry. 2020. "Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re) Insurers and Likes". *IEEE Internet of Things Journal* 8(9).

Pal, R., P. Liu, T. Lu, and E. Y. Hua. 2022. "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* 6(4).

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. IEEE.

Pal, R., K. Psounis, J. Crowcroft, F. Kelly, P. Hui, S. Tarkoma, A. Kumar, J. Kelly, A. Chatterjee, L. Golubchik 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.

Peng, C., M. Xu, S. Xu, and T. Hu. 2018. "Modeling Multivariate Cybersecurity Risks". *Journal of Applied Statistics* 45(15):2718–2740.

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

Romanosky, S., L. Ablon, A. Kuehn, and T. Jones. 2019. "Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?". *Journal of Cybersecurity* 5(1). tyz002.

Shetty, N., G. Schwartz, M. Felegyhazi, and J. Walrand. 2010a. "Competitive Cyber-insurance and Internet Security". In *Economics of Information Security and Privacy*, 229–247. Springer.

Shetty, N., G. Schwartz, M. Felegyhazi, and J. Walrand. 2010b. "Competitive Cyber-insurance and Internet Security". In *Economics of Information Security and Privacy*, 229–247. Springer.

Vasicek, O. 1977. "An Equilibrium Characterization of the Term Structure". *Journal of financial economics* 5(2):177–188.

Vaugirard, V. E. 2003. "Valuing Catastrophe Bonds by Monte Carlo Simulations". *Applied Mathematical Finance* 10(1):75–90.

Wheatley, S., A. Hofmann, and D. Sornette. 2021. "Addressing Insurance of Data Breach Cyber Risks in the Catastrophe Framework". *The Geneva Papers on Risk and Insurance-Issues and Practice* 46(1):53–78.

Wheatley, S., T. Maillart, and D. Sornette. 2016. "The Extreme Risk of Personal Data Breaches and the Erosion of Privacy". *The European Physical Journal B* 89(1):1–12.

Wolff, J. 2022. *Cyber-insurance Policy: Rethinking International Risk for the Internet Age*. MIT Press.

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 Cybersecurity at MIT Sloan (CAMS) at the MIT Sloan School of Management. His primary research interest lies in developing interdisciplinary and quantitative cyber risk/resilience management solutions for IT/IoT driven enterprises. Ranjan is an Associate Editor of the ACM Transactions of MIS. 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 and logistics in energy and transportation systems, and cyber-security. He has been a consultant to organizations such as The World Bank an Deloitte Touche Tohmatsu. His email is bnag@iimcal.ac.in.