Systemic Cyber Attacks and Currency Pressure: Financial Market Infrastructure as a Channel for Global Fragmentation

Ilias Chiboub*

Abstract

I model a global coordination game between a state-sponsored attacker targeting financial market infrastructures (FMI) and a continuum of foreign investors whose capital allocation decisions determine exchange market pressure (EMP). I empirically test the resulting theoretical propositions using a Double Machine Learning Local Projections framework on a panel of 30 emerging markets from 2015 to 2024. Results reveal a severe nonlinear macroeconomic vulnerability. I demonstrate that moderate FMI cyber attacks are smoothly absorbed by institutional buffers; under these conditions, foreign investors default to rational inattention and hold their positions, resulting in a negligible exchange market response. In contrast, extreme tail-risk cyber attacks (99th percentile) weaken this resilience and trigger a panicked first-mover advantage dynamic. Fearing institutional liquidity freezes, foreign investors rapidly liquidate emerging market exposure, generating an immediate, massive surge in exchange market pressure. This asymmetric flight-to-safety actively fractures emerging market integration as capital retreats to core-market safe havens. Ultimately, these findings establish that emerging markets are structurally forced to absorb the macroeconomic fallout of FMI cyber shocks, severely exacerbating cross-border financial fragmentation and contagion.

Keywords: Systemic cyber risk, Exchange market pressure, Financial market infrastructure, Global games, Causal machine learning, Emerging markets

JEL Classification: F31, F32, G15, C72, C55, E58

*PhD Candidate, Mohammed V University in Rabat. Email: ilias_chiboub@um5.ac.ma. Address: Avenue Mohammed Ben Abdallah Ragragui Al Irfane, 6430, Rabat, Morocco.

No external funding was received for this project.

1 Introduction

The rapid digitization of global financial infrastructure has elevated cyber risk into a primary threat to macroeconomic stability, capable of triggering severe financial contagion (Kopp et al., 2017; Adelmann et al., 2020; Doerr et al., 2022). Systemic cyber incidents can halt payment execution or compromise ledger integrity across vital interbank settlement networks. In the resulting informational opacity, market participants cannot distinguish in real time between temporary operational paralysis and fundamental counterparty insolvency, triggering preemptive liquidity hoarding and credit freezes (IMF, 2024a; OECD, 2026). Because the interconnected architecture of global finance relies on a few critical chokepoints (e.g., SWIFT, CLS Bank, Fedwire, Euroclear, and the DTCC), an attack targeting a single central node forces these networks to delay settlement chains or temporarily sever cross-border connections. These settlement failures can quickly evolve into diminished market confidence and cross-border capital flight. For central banks, these incidents are no longer viewed merely as isolated IT failures, but rather as systemic macro-financial risks capable of generating massive economic losses (Doerr et al., 2022). Yet, while the literature extensively emphasizes how cyber attacks destabilize micro-level banking firms (Eisenbach et al., 2022; Pollmeier et al., 2023; Gaies et al., 2026), our understanding of how catastrophic cyber shocks targeting financial market infrastructures (FMI) interact with aggregate exchange rates remains critically limited.

More importantly, the rise of state-sponsored cyber attacks introduces a potent instrument of gray-zone economic warfare designed to induce currency attrition (Crespo, 2018). Such attacks have surged in tandem with recent geopolitical conflicts (IMF, 2024a). Unlike conventional criminal intrusions seeking short-term financial extraction, state-sponsored campaigns frequently deploy sophisticated zero-day exploits and distributed denial-of-service operations to covertly disrupt critical payment architectures over extended horizons (Singh, 2025). These attacks convert transitory operational disturbances into structural macro-financial shocks. Under this cyber-induced distress, foreign investors face severe loss uncertainty, amplifying risk aversion and triggering sudden capital flight. Because this rapid capital drain exerts intense pressure on the currency, the exchange rate depreciates rapidly, accelerating cross-border financial fragmentation by fueling sovereign risk premia and severing emerging market borrowers from international funding rails. I therefore investigate a central question for financial stability: how do systemic cyber attacks targeting global financial market infrastructures transmit into exchange market pressure in emerging markets?

This question carries substantial implications for foreign investors, financial institutions, and sovereign authorities. Under covert and high-velocity cyber attacks, verifying account balances and liquidity solvency requires time-intensive forensic audits. This fragments the market's knowledge base and obscures fundamental data. When a threat compromises infrastructure bottlenecks, it fundamentally alters the coordinated

behavior of foreign investors, forcing them to rapidly toggle between filtering out the operational noise via rational inattention (Sims, 2003) or executing a first-mover advantage to escape the impending liquidity shock (Bernardo and Welch, 2004).

To formalize these dynamics, I develop a global coordination game (Morris and Shin, 1998; Frankel et al., 2003) between two strategic actors: a foreign state-sponsored attacker and a continuum of foreign investors. To empirically evaluate the resulting theoretical mechanisms, I utilize a panel of 30 emerging market economies spanning 2015 to 2024, merging monthly data on systemic FMI cyber attacks with a constructed Exchange Market Pressure (EMP) index. Estimating the macroeconomic transmission of these shocks poses a severe identification challenge: traditional linear models struggle with high-dimensional confounders, while naive machine learning approaches introduce heavy regularization bias. To execute robust causal identification, I employ a Double Machine Learning with Local Projections (DML-LP) framework (Jordà, 2005; Chernozhukov et al., 2018) utilizing double residualization.

The empirical analysis establishes three core transmission mechanisms:

- **Operational Buffering and Rational Inattention:** Institutional resilience absorbs low-to-moderate cyber attacks that fall below a salient critical threshold. Backup systems ensure continuous payment settlements, and mandated intraday recovery protocols prevent long-duration disruptions. Consequently, exchange market pressure remains dormant as foreign investors hold their positions, rationally filtering out standard operational frictions as benign noise.

- **Informational Opacity and First-Mover Advantage:** Breaching the catastrophic 99th-percentile tail-risk threshold compromises critical infrastructure networks, generating severe uncertainty regarding institutional solvency. Fearing that their claims will be indefinitely trapped inside a frozen clearinghouse or central securities depository, foreign investors execute preemptive capital flight. This synchronized panic generates an immediate, massive surge in exchange market pressure.

- **Asymmetric Fragmentation and Flight-to-Safety:** Under extreme systemic cyber attacks, foreign investors and multinational banks derisk their portfolios by dumping high-beta peripheral emerging market assets and rushing toward the highly liquid US dollar. Even though the targeted FMIs are physically concentrated within advanced economies, this geographic asymmetry forces emerging markets to absorb the macroeconomic fallout, severely exacerbating global financial fragmentation.

In relation to the literature, I make four distinct contributions at the intersection of international finance, cyber risk, game theory, and causal machine learning.

First, I extend the emerging macro-finance literature on cyber risk. While existing discussions regarding cyber threats and currencies remain largely descriptive and anecdotal (Crespo, 2018), the empirical

literature has predominantly focused on firm-level banking impacts (Eisenbach et al., 2022; Gaies et al., 2026) or decentralized finance (Caporale et al., 2020; Tian et al., 2023). I bridge this gap by establishing the first formal game-theoretic and causal empirical framework that models systemic cyber attacks targeting FMIs as macroeconomic shocks transmitting directly into exchange market pressure.

Second, I empirically quantify the non-linear macroeconomic vulnerability of the global financial system. While FMIs exhibit resilience against routine attacks, I demonstrate that catastrophic historical tail-risk events weaken this resilience, generating a massive surge in exchange market pressure across the emerging market periphery. This confirms the premise held by central banks that network interconnectedness serves as a primary transmission channel for cross-border liquidity retrenchment under cyber threats (Doerr et al., 2022; IMF, 2024a; OECD, 2026).

Third, consistent with the literature on investor risk management (Sims, 2003; Bernardo and Welch, 2004), I demonstrate that the dominant strategy of financial investors shifts violently from rational noise filtering to a panicked first-mover advantage based purely on the intensity threshold of the FMI cyber attack. I formally extend the foundational literature on exchange market pressure (Krugman, 1979; Eichengreen et al., 1994; Obstfeld, 1996). While these canonical currency crisis models focus primarily on sovereign insolvency or shifting macroeconomic fundamentals, my framework introduces systemic geoeconomic shocks as a novel, independent trigger for exchange market pressure.

Fourth, I advance the empirical literature on macroeconomic shock identification (Auerbach and Gorodnichenko, 2012; Ramey and Zubairy, 2018) by bridging game-theoretic modeling with causal machine learning. Moving beyond restrictive linear structures, I deploy a highly flexible DML-LP framework. I embed a Mundlak transformation (Mundlak, 1978) directly into the machine learning first-stage nuisance equations to rigorously handle unobserved country-level heterogeneity within a nonlinear setting. This advanced semi-parametric approach effectively isolates the nonlinear asymmetries inherent in shock propagation while entirely mitigating high-dimensional regularization bias.

Understanding this cyber risk transmission channel carries profound implications for international macro-finance and systemic risk. Specifically, these findings reveal a harsh geoeconomic reality: sophisticated, state-sponsored cyber campaigns targeting international settlement networks generate profound cross-border spillover and currency risks, completely independent of the domestic macroeconomic fundamentals of the emerging markets they damage. Ultimately, isolated and heavily sanctioned economies can exploit these FMI vulnerabilities to intensify global financial fragmentation.

The remainder of the paper is organized as follows. Section 2 models the theoretical framework and solves the global game. Section 3 introduces the data and summary statistics. Section 4 presents the DML-LP empirical strategy. Section 5 discusses the empirical results and mechanism verifications. Finally, Section

6 concludes.

2 The Game Theory Model

2.1 Game structure and players

I model a global coordination game (Morris and Shin, 1998; Frankel et al., 2003) in which a foreign, state-sponsored attacker launches systemic cyber attacks against critical financial market infrastructures (FMI) (e.g., SWIFT, CLS Bank, Fedwire, Euroclear, DTCC). The attacker's objective is to maximize multi-vector geoeconomic gain, primarily by provoking core-periphery financial fragmentation and extracting hard currency to bypass international sanctions. Regardless of whether the attacker's motive is strategic disruption or direct financial theft, emerging market foreign exchange venues are forced to structurally absorb the resulting operational shocks.

This game-theoretic approach is essential for formally capturing the strategic incentives, information asymmetries, and Bayesian belief formations that characterize modern financial crises. Because state-sponsored cyber attacks operate covertly, they generate severe real-time uncertainty regarding the true aggregate impairment of global clearinghouses and central securities depositories. In this opaque environment, market participants must coordinate their liquidity responses, generating intense strategic complementarities.

Crucially, the interaction among investors depends heavily on the severity of the infrastructure shock. Standard multiple-equilibrium macroeconomic models fail to capture this dynamic precisely because they lack a mechanism to predict when a panic will occur. The global game framework resolves this uncertainty. By introducing small, idiosyncratic private noise regarding the severity of the operational disruption, the framework collapses the multiple equilibria into a unique, monotone threshold equilibrium (θ^*). This allows the model to map the unobserved state of financial infrastructure directly to the observable onset of a currency run.

I assign two active strategic players and a mechanical institutional defender to capture the coordination dynamics of a systemic FMI freeze. The game unfolds over a single critical window (t):

- **Player 1 (Foreign State-Sponsored Attacker):**

  Action: Chooses the intensity of the cyber attack targeting the FMI, which generates an underlying operational disruption state $\theta \in [0, \bar{\theta}]$ (empirically proxied by the count of systemic FMI cyber attacks)
  Payoff: Maximizes utility U_{FA} in Equation (1), where Ω represents the multi-vector geoeconomic and hard-currency extraction gain for inducing Exchange Market Pressure (EMP_t), and $c(\theta)$ captures the

economic costs and attribution risks of the offensive campaign.

$$U_{FA}(\theta) = \Omega \cdot \mathbb{E}[EMP_t] - c(\theta) \tag{1}$$

- **Player 2 (Continuum of Foreign Investors):**

  Action: A continuum of foreign investors, indexed by $i \in [0, 1]$, simultaneously choose an action under the set $\kappa_i \in \{\text{Hold}, \text{flee}\}$. The aggregate mass of investors who choose to run is denoted by $l \in [0, 1]$.

  Payoff: Investors optimize their expected portfolio returns based on their private information set. Fleeing ensures a safe-haven return normalized to 0. Holding the position yields a positive return $r > 0$ if the FMI continues settling transactions successfully. However, if the system freezes due to the combined stress of the systemic cyber attack (θ) and the aggregate capital flight (l), holders suffer a severe liquidity lock-up penalty $-C_{trap}$, as expressed in Equation (2):

$$U_{FI}(\text{Hold}) = \begin{cases} r & \text{if FMI survives} \\ -C_{trap} & \text{if FMI freezes} \end{cases} \tag{2}$$

- **The institutional defender:**

  Mechanism: Instead of acting as a strategic player, the financial market infrastructure plumbing and the central bank act as a mechanical structural buffer (operationalized through standby RTGS protocols, cyber recovery frameworks, and central bank liquidity facilities). The system successfully clears settlement transactions if and only if the combination of the cyber disruption state (θ) and the mass of fleeing investors (l) is strictly less than the system's structural capacity K. A systemic freeze (and subsequent EMP surge) occurs when $\theta + l \geq K$.

2.2 Timing and information asymmetry

To eliminate the multiple equilibria endemic to standard exchange market pressure models, the flow of information is opaque. Investors are uncertain about the true state of the cyber disruption (θ) in real time due to institutional silence and network latency. The timing proceeds as follows:

1. **Attack initialization:** The attacker selects the intensity of the FMI cyber attack θ.

2. **Noisy signal observation:** Nature draws an idiosyncratic noise term $\epsilon_i \sim U[-\varepsilon, \varepsilon]$ for each investor i. Only a private, noisy signal of the network's true impairment is observed by each foreign investor:

$x_i = \theta + \epsilon_i$. Where different financial institutions have asymmetric visibility into clearinghouse backlogs based on their specific counterparty exposures.

3. **Simultaneous action:** Based on their private signal x_i, each investor updates their Bayesian belief about both the true state of the attack (θ) and the likely actions of all other investors (l), simultaneously choosing whether to Hold or flee.

4. **Threshold realization:** Aggregate actions are computed. If the cyber attack intensity is low-to-moderate and few foreign investors flee, the institutional buffer is maintained ($EMP_t = 0$). If the intensity of the cyber attack is extreme and triggers coordinated flight ($\theta + l \geq K$), the system freezes, generating a severe macro-financial currency pressure ($EMP_t \gg 0$) and rewarding the cyber attacker.

2.3 Equilibrium solution and propositions

This global coordination game is solved via the Iterated Elimination of Strictly Dominated Strategies (IESDS) (Morris and Shin, 1998).

Upon observing the private, noisy signal x_i, each foreign investor dynamically updates their posterior belief regarding the true severity of the cyber disruption (θ) and the anticipated mass of fleeing investors (l). The foreign investor calculates the conditional probability of whether the financial market infrastructure can freeze, defined as the state where the combined cyber shock and capital flight exceed the system's capacity and buffers (K):

$$\mu(x_i) = \Pr(\text{FMI Freezes} \mid x_i) = \Pr(\theta + l \geq K \mid x_i) \tag{3}$$

Because the payoff structure exhibits one-sided strategic complementarity (the incentive to flee increases as more investors flee), the expected utility function of holding is mechanically decreasing in x_i. Consequently, the IESDS process converges to a unique, symmetric shifting strategy around a critical signal threshold x^*:

$$\kappa_i(x_i) = \begin{cases} \text{flee} & \text{if } x_i \geq x^* \\ \text{Hold} & \text{if } x_i < x^* \end{cases} \tag{4}$$

Aggregating these individual strategies yields a unique critical threshold θ^* for the true operational state. If the cyber attacks intensity is below this threshold ($\theta < \theta^*$), the mass of fleeing investors is insufficient to break the structural buffer K, and the system holds without macro-financial consequence. However, if the cyber attacks intensity breaches the critical ($\theta \geq \theta^*$), it spark a synchronized, self-fulfilling liquidity run

that induce an infrastructural freeze.

This theoretical cutoff θ^* provides the direct micro-foundation for the nonlinear, 99th-percentile extreme empirical threshold (D_t^{tail}) evaluated in the causal machine learning framework.

The strategic interactions within this Global Game yield a unique threshold equilibrium. The utility functions of the players shape the equilibrium path, generating three core theoretical propositions that map directly to the empirical identification strategy:

- **Proposition 1 (Operational buffering and rational inattention):** $\beta_{\text{EMP}} = 0$

  When systemic cyber attacks targeting financial market infrastructure fall below a critical operational threshold ($D_t < \theta^*$), they fail to transmit into macroeconomic exchange market pressure. Because modern financial networks maintain sufficient structural redundancies, such as standby Real-Time Gross Settlement (RTGS) protocols and offline data vaults, to bypass minor transmission delays. Furthermore, central bank intraday liquidity facilities easily absorb clearing backlogs without risking the solvency of domestic banks. Under these conditions, foreign investors filter out this noise and have no incentive to incur the transaction costs of cross-border portfolio allocations over transient operational frictions. By choosing to hold ($\kappa_t = \text{Hold}$), investors anchor aggregate beliefs ($\mu_t \approx \mu_0$), leaving net exchange market pressure statistically indistinguishable from zero. With no capital flight to combat, central bank intervention losses are averted. Because $\mathbb{E}[EMP_t] = 0$, the expected payoff of the state-sponsored attacker collapses to $U_{FA} = -c(D_t) < 0$, strictly deterring geoeconomic attacks below the salience threshold.

- **Proposition 2 (Informational opacity and first-mover advantage):** $\beta_{\text{EMP}} > 0$

  When systemic cyber attacks breach the extreme operational threshold ($D_t \geq \theta^*$), the core networks for cross-border trade settlement are severely compromised. Market participants cannot distinguish between solvent and insolvent settlement nodes in real time, triggering immediate liquidity hoarding. To avoid having their claims indefinitely trapped inside a frozen clearinghouse or central securities depository, the strictly dominant strategy for foreign investors is preemptive capital flight ($\kappa_t = \text{Run}$) before settlement rails seize completely. This coordinated exit drastically amplifies exchange market pressure. The resulting reserve drain imposes heavy intervention costs on the central bank and accelerates Bayesian belief updating toward an impending currency crisis ($\mu_t \to 1$), creating a self-fulfilling speculative pressure. At this extreme threshold, the macroeconomic response becomes sharply nonlinear. The attacker realizes a positive net payoff, $U_{FA}(D_t) = \Omega \cdot \mathbb{E}[\text{EMP}_t] - c(D_t) > 0$, incentivizing future tail-risk strikes.

- **Proposition 3 (Core-periphery fragmentation and asymmetric flight-to-safety):** $\beta_{\text{EMP}} \gg 0$

Although critical financial market infrastructures are heavily centralized within advanced economies (e.g., SWIFT, CLS Bank, Fedwire, Euroclear), severe cyber attacks generate highly asymmetric exchange market pressure on emerging markets. Confronted with the threat of trapped liquidity, foreign investors reflexively retrench from high-beta peripheral assets and rush toward highly liquid safe havens, such as US sovereign debt. Simultaneously, parent multinational dealer banks headquartered in the advanced core rapidly recall liquidity from their emerging market subsidiaries, severing cross-border interbank funding and financial integration. If the attacking state is already heavily sanctioned or financially isolated from the advanced core, it suffers no reciprocal capital flight. This isolation amplifies its relative geoeconomic gain ($U_{FA} \gg 0$) and exacerbates financial fragmentation.

3 Data and Summary Statistics

3.1 Sample and timeframe

To empirically evaluate the propositions of the game-theoretic model, I construct a panel of 30 emerging market economies observed monthly from 2015 to 2024 ($T = 120$). Emerging markets provide an ideal laboratory for this analysis; unlike advanced safe-haven economies, they exhibit high structural exposure to sudden capital flight and currency volatility. The sample incorporates a geographically diverse cross-section from Africa, Asia, Eastern Europe, Latin America, and the Middle East, ensuring the empirical estimates capture global macro-financial dynamics rather than localized regional trends. To maintain sample homogeneity and identification rigor, I exclude countries experiencing extreme extra-economic dislocations, such as physical war mobilization, total institutional collapse, or severe structural data gaps. This ensures that variations in domestic exchange market pressure (EMP_{it}) are not confounded by isolated physical war campaigns or severe economic sanctions.

Crucially, while the outcome variable (EMP_{it}) is measured at the country-month level, the primary treatment variable (D_t) is constructed as an aggregate global index of systemic cyber shocks to Financial Market Infrastructure (FMI). Modern finance relies on a highly centralized network of institutional chokepoints, such as SWIFT, CLS, Fedwire, and TARGET2, to settle trillions of dollars in daily cross-border transactions. Because of this deep structural interconnectivity, cyber disruptions at these critical nodes generate massive spillover risks, transmitting liquidity shocks through the global financial system even if a specific emerging market is not the direct target. By defining the shock as a globally aggregated phenomenon, the research design naturally mitigates domestic endogeneity and reverse causality concerns. The timing of an attack on global clearinghouses is strictly exogenous to the internal macroeconomic vulnerabilities and

idiosyncratic data opacity of any individual emerging market in the panel.

The timeframe from 2015 to 2024 captures a critical geoeconomic epoch defined by an unprecedented escalation in state-sponsored cyber operations and sophisticated infrastructure targeting. Because systemic cyber attacks are inherently high-velocity and episodic, a monthly data frequency is required to accurately capture their immediate macro-financial footprint. The strict exogeneity of these global shocks provides a clean empirical environment to identify their causal transmission into emerging market currency stress.

3.2 Construction of the exchange market pressure index

To track financial market stress triggered by shifts in the supply and demand for foreign currency, traditional balance-of-payments (BoP) metrics are inadequate. While BoP data captures asset liquidation and portfolio re-allocation, it relies on delayed, low frequency reporting that overlooks evasion methods, disguised transactions, and unobservable central bank defense mechanisms. Conversely, relying solely on nominal exchange rate movements is similarly flawed, as central banks under fixed regimes actively defend a pegged rate by depleting foreign reserves. To overcome these limitations, I construct a standardized Exchange Market Pressure (EMP) index following the classic speculative attack framework (Girton and Roper, 1977; Eichengreen et al., 1994). This measures the net shadow supply and demand for foreign currency generated by capital flows, regardless of the explicit exchange rate regime. As specified in Equation (5):

$$EMP_{it} = \frac{\Delta e_{it}}{\sigma_{\Delta e,i}} - \frac{\Delta R_{it}}{\sigma_{\Delta R,i}} + \frac{\Delta r_{it}}{\sigma_{\Delta r,i}} \tag{5}$$

where Δe_{it}: the percentage monthly change in the nominal exchange rate (depreciation > 0)
ΔR_{it}: the percentage monthly change in total foreign exchange reserves (depletion < 0)
Δr_{it}: the monthly change in the policy interest rate.

The index is constructed as a variance-weighted combination of nominal exchange rate movements (Yahoo Finance, 2025), foreign exchange reserve changes (IMF, 2024b), and short-term interest rate shifts (BIS, 2024). Each component is weighted by the inverse of its country-specific standard deviation to equalize unit variances and prevent the most volatile series from dominating the index. I utilize 2014 as a pre-sample buffer to compute initial monthly changes but calculate the standard deviations strictly over the active 2015-2024 estimation window.

3.3 Construction of the systemic FMI cyber attack metric

I quantify systemic cyber shocks targeting financial market infrastructure (FMI) at a monthly frequency using event data from the Center for Governance of Technology and Systems (GoTech) and the Center

for International and Security Studies at Maryland (CISSM) at the University of Maryland (Harry and Gallagher, 2018). This database is increasingly recognized in the macro-finance literature and has been deployed by institutions such as the World Bank Group, the European Central Bank, and the International Monetary Fund (Khiaonarong and Zheng, 2026). The underlying database extracts high-frequency cyber incidents from open-web and dark-web sources by combining automated web-scraping algorithms with the GDELT Project's Web News NGrams 3.0 Dataset, analyzing millions of news articles across more than 60 languages.

Because the raw dataset aggregates thousands of routine cyber incidents across all economic sectors, employing an unfiltered count would severely confound the empirical mechanism with operational noise and bias the estimates toward zero. To isolate true systemic macro-financial shocks on critical global nodes from localized, idiosyncratic corporate disruptions, I construct the primary treatment variable (D_t) by applying a systematic, multi-layered lexical filter to the CISSM database. The filtering procedure follows a highly restrictive, four-step identification protocol:

First, I restrict the initial search space to the "Finance" and "Public Administration" sectors to accurately capture commercial banks, central banks, and clearinghouses. Within this subset, the filter evaluates target organization names and event descriptions against a meticulously curated taxonomy of systemic nodes. This taxonomy is structured around four critical pillars of the global financial market infrastructure (FMI), presented in Table 1:

Table 1: Taxonomy of Systemic Financial Market Infrastructure

Infrastructure Category	**Lexical Search Terms**
Baseline Cash & FX Rails	SWIFT, Central Bank, Clearinghouse, Clearing, Fedwire, Target2, CLS, Interbank, Reserve Bank, Financial Settlement, RTGS, IMF, Bank for International Settlements, CHIPS
Geoeconomic & Alternative Rails	CIPS, SPFS, ISO 20022
Securities, Collateral, & CSD Hubs	CSD, ICSD, Euroclear, Clearstream, DTCC, NSCC, CCP, Central Counterparty
Systemic Technology Providers	ION Cleared, ION Group, Core Banking Provider, Fiserv, Financial Market Infrastructure

Notes and Source: Author keyword taxonomy applied to raw records from the University of Maryland CISSM Cyber Events Database. Parsing enforces strict regex word boundaries to prevent false-positive substring matches, supplemented by exclusionary filters for incidents outside the systemic macro-financial network.

Second, to eliminate false positives caused by substring capture in the textual data, the parsing algorithm enforces exact regular expression word boundaries (`\b`). This strict boundary enforcement ensures, for example, that a search for the Bank for International Settlements ("BIS") isolates the actual institution rather than capturing unrelated cyber incidents involving string matches such as the municipality of

"Biscayne" or the cryptocurrency exchange "Bisq".

Third, to further guarantee the macro-financial purity of the metric, I apply a secondary exclusionary filter. This step actively removes incidents involving organizations that share financial terminology but operate entirely outside the systemic macro-financial network (e.g., student clearinghouses, or medical and retirement payment portals).

Fourth, I aggregate the curated discrete events into a monthly time series. Months with zero systemic infrastructure cyberattacks are explicitly coded as zeros rather than treated as missing values. This prevents sample attrition and preserves both the continuous lag structure and the time fixed effects required by the local projections framework.

The CISSM cyber events database captures a comprehensive spectrum of attack vectors that encompass (a) external denial-of-service attacks (e.g., BGP hijacking, ICMP/SYN floods, and Ping of Death); (b) message and interface manipulation (e.g., website defacement and account hijacking); (c) internal denial-of-service events (e.g., core router resets and server malware installations); (d) data disruption (e.g., wiper viruses, ransomware, and data manipulation); and (e) physical hardware attacks (e.g., programmable logic controller manipulation and industrial control system intrusions).

3.4 Macroeconomic and cyber security controls

To control for macroeconomic performance without introducing look-ahead bias, I extract quarterly real GDP series from the IMF (IMF, 2024c), and compute year-over-year percentage changes. The resulting quarterly growth rate is mapped into monthly observations via step-wise forward-filling (zero-order hold) to eliminate seasonal noise. I also incorporate monthly inflation rates (Ha et al., 2023) and policy interest rates from the Bank of International Settlements (BIS, 2024).

To determine the exchange rate regimes of the panel sample, I utilize the International Monetary Fund's de facto classification system (IMF, 2025). To prevent overfitting and under-representation arising from the sparse distribution of observations across sub-categories, I consolidate the arrangements into a binary time-variant framework. The fixed exchange rate regime class ($Regime_{i,t} = 0$) includes hard pegs, soft pegs, and intermediate managed residual arrangements. The floating regime class ($Regime_{i,t} = 1$) accounts for both free and managed floats. Instead of relying on static country classifications, I leverage monthly dynamic classifications to capture within-country regime transitions and policy failures, eliminating misclassifications bias.

To control for cross-sectional baseline variances in domestic cyber security readiness, I extract the Global Cyber security Index (GCI) (ITC, 2015, 2018, 2021, 2024) from the International Telecommunication

Union. Because this index is reported triennially and frequently updates its survey methodology, applying linear interpolation across monthly observations would introduce artificial measurement biases. Instead, I construct a time-invariant, country-level baseline score ($\overline{GCI}_i$) defined as the historical mean score for unit i. As weaker cyber infrastructure amplifies the localized impact of a global shock, controlling for domestic cyber security capacity alongside macro-financial conditions is crucial to prevent omitted variable biases.

I include the CBOE Volatility Index (VIX) and the federal funds rate (Chicago Board Options Exchange, 2024; Board of Governors of the Federal Reserve System (US), 2024) to control for global financial conditions. These variables serve as standard proxies for international risk aversion, global market sentiment, and US monetary policy stance.

3.5 Summary statistics

Table (2) presents the summary statistics for the 30 emerging market economies observed from 2015 to 2024:

Table 2: Summary Statistics (2015 to 2024)

Variable	**Obs**	**Mean**	**SD**	**Min**	**Max**
Panel A: Outcome and EMP Components					
Exchange Market Pressure, Z-Score (EMP)	3,419	0.066	1.897	−8.392	10.544
Nominal Depreciation (% MoM, Δe)	3,600	0.519	4.256	−15.354	124.463
Foreign Reserves Growth (% MoM, ΔR)	3,421	0.435	5.092	−57.807	122.078
Policy Rate Change (pp, Δr)	3,598	0.034	1.337	−33.000	22.868
Panel B: Cyber Shock and Macroeconomic Controls (W_{it})					
Systemic FMI Cyber Attacks (D)	3,600	0.600	1.868	0.000	19.000
Global Cybersecurity Index ($\overline{GCI}_i$)	3,600	−0.012	0.860	−3.256	1.188
Inflation Rate (% per annum)	3,564	0.562	1.284	−6.467	25.466
Real GDP Growth Rate (% YoY)	3,570	3.106	5.556	−31.394	52.060
Exchange Rate Regime	3,600	0.638	0.481	0.000	1.000
VIX CBOE	3,600	18.258	6.646	10.130	57.740
FEDFUNDS Rate (% MoM)	3,600	0.036	0.182	−0.930	0.700

Notes: The panel spans 30 emerging markets observed monthly from 2015 to 2024. To prevent data loss, 2014 data was utilized to calculate variation rates in 2015. Minor fluctuations in observation counts across variables reflect historical reporting gaps. The Systemic FMI Cyber Attacks variable (D) isolates disruptive incidents targeting critical financial market infrastructures. Source: Author calculations.

Table 2 presents the summary statistics for the estimation sample. The panel structure provides substantial statistical power for the local projections framework, yielding well over 3,000 observations per regression horizon to ensure robust, country-clustered standard errors. The primary dependent variable, the Exchange Market Pressure (EMP) index, exhibits a sample mean of 0.067 and a standard deviation of 1.921, confirming sufficient time-series and cross-sectional variation to capture periods of severe currency stress.

Crucially, the primary treatment variable, systemic FMI cyber shocks (D), records a mean of 0.600

incidents with a standard deviation of 1.868. This right-skewed distribution highlights the episodic, tail-risk nature of systemic cyber threats. The maximum observed value of 19 concurrent incidents coincides with May 2016, a historic epoch of intense cyber activity and breaches. This cluster aligns with the widespread public disclosure of a highly coordinated, state-sponsored campaign targeting the SWIFT transfer network and international settlement accounts across Bangladesh, Vietnam, and Ecuador (Reuters Editorial, 2016; Finkle and Wagstaff, 2016; Maurer and Nelson, 2021). This unprecedented wave of cyber attacks empirically demonstrates that vulnerabilities in centralized financial market infrastructure generate profound cross-border spillover risks, independent of the domestic macroeconomic fundamentals of the emerging markets in this panel.

Finally, the standardized baseline Global Cybersecurity Index ($\overline{GCI}_i$) exhibits a mean of -0.012 and a standard deviation of 0.860. The negative mean indicates that, on average, the emerging markets in this sample possess weaker institutional cybersecurity readiness relative to the global baseline. Because this structural divergence could amplify a country's susceptibility to global contagion, this metric is strictly partialled out within the first-stage Double Machine Learning (DML) algorithms to prevent omitted variable bias.

Detailed definitions and sources for all variables are cataloged in Table (7) in the Appendix (A.1).

4 Empirical Identification Strategy

To empirically test the game-theoretic propositions, I employ a Double Machine Learning Local Projections (DML-LP) approach. Standard linear panel specifications fail to capture the nonlinear, high-velocity, and asymmetric transmission of operational cyber shocks to financial markets, often suffering from severe endogeneity and model misspecification bias. To overcome these limitations, I integrate double machine learning (Chernozhukov et al., 2018) with local projections (Jordà, 2005), employing a random forest learner (Breiman, 2001) to estimate the nuisance parameters.

This DML-LP strategy bypasses the necessity of defining rigid, binary treatment-control groups by constructing continuous counterfactual treatment residuals. Furthermore, the flexibility of the LP impulse responses allows for the seamless integration of non-parametric residuals generated via DML, exhibiting significant robustness to model misspecification compared to traditional structural models.

4.1 First-stage DML and double residualisation

To isolate the causal effect of cyber attacks on the Exchange Market Pressure index (EMP_{it}), I employ a double residualization procedure that purifies both the treatment and the outcome from high-dimensional,

nonlinear macroeconomic confounders. By satisfying Neyman orthogonality (Chernozhukov et al., 2018), this approach minimizes selection and endogeneity biases without relying on infeasible or weak instrumental variables across a heterogeneous panel of 30 emerging markets.

To guarantee strict pre-treatment exogeneity, eliminate simultaneity bias, and prevent reverse causality, all macroeconomic covariates and policy indicators are lagged by one period $(t-1)$. Furthermore, rather than incorporating standard high-cardinality country fixed effects, which are known to cause severe overfitting and mechanically absorb treatment variation in machine learning estimations, I embed the Correlated Random Effects (CRE) transformation (Mundlak, 1978) directly within the first-stage nuisance equations, following the framework developed by Chiboub and Sadok (2026). This CRE framework strictly models unobserved, time-invariant country heterogeneity by including the country-specific temporal averages of all time-varying controls.

To rigorously address the potential for omitted variable bias driven by the global macroeconomic environment, the model employs a dual-control strategy. Because the catastrophic cyber shock (D_t) operates as a purely global treatment variable, the inclusion of standard year-month time dummies would induce perfect multicollinearity and absorb the primary structural variance of the shock. To circumvent this standard panel identification challenge, the model first retains seasonal month-of-the-year fixed effects to capture cyclical global liquidity fluctuations (such as end-of-year repo market stress or tax season anomalies) without destroying the global time series.

Second, the Double Machine Learning (DML) architecture explicitly ingests two critical global "push factors" alongside the domestic macroeconomic controls. Specifically, I incorporate the lagged CBOE Volatility Index (VIX) to proxy for the Global Financial Cycle, capturing high-frequency shifts in global risk aversion and market sentiment (Rey, 2015). I also incorporate the lagged first difference of the US Federal Funds Rate to rigorously control for US monetary policy tightening cycles. This high-dimensional conditioning allows the first-stage Random Forest algorithms to non-parametrically partial out the influence of overarching global macro-financial shocks without relying on naive linear time dummies.

The first-stage DML nuisance equations are estimated over the high-dimensional feature vector W_{it} defined in Equation (6):

$$W_{it} = \left[\mathbf{Z}_{i,t-1}, \ldots, \mathbf{Z}_{i,t-p}, \overline{\mathbf{Z}}_i, \overline{GCI}_i, \text{Season}_t\right] \tag{6}$$

Where $\mathbf{Z}_{i,t-1}$ is the vector of one-period lagged macroeconomic control variables (real GDP growth rates, inflation rates, CBOE Volatility Index (VIX), the first difference of the US Federal Funds Rate, exchange rate changes, and foreign exchange reserves changes).

$\mathbf{Z}_{i,t-p}$ represents country-specific historical pre-treatment lags up to order $p = 3$.

$\overline{\mathbf{Z}}_i = T^{-1} \sum_{t=1}^{T} \mathbf{Z}_{it}$: the unit-specific temporal means of the control variables (Mundlak correlated random effects terms).

$\overline{GCI}_i$ represents the time-invariant baseline Global Cybersecurity Index.

Season_t is the vector of seasonal month-of-the-year fixed effects.

4.2 Baseline specification

In the baseline framework, the primary systemic cyber shock D_t is modeled as a continuous count of global incidents. For each forward horizon $h \in \{0, 1, \ldots, 5\}$, the nuisance equations for both the outcome and the treatment variable are estimated via 5-fold cross-fitting ($K = 5$) using Random Forest regressors ($n_{\text{tree}} = 100$, max_depth = 3) (Breiman, 2001). These hyperparameters restrict tree depth to prevent overfitting and optimize predictive power in Equations (7) and (8):

$$Y_{i,t+h} = g_0^h(W_{it}) + U_{i,t+h}^h, \quad \mathbb{E}[U_{i,t+h}^h \mid W_{it}] = 0 \tag{7}$$

$$D_t = m_0(W_{it}) + V_t, \quad \mathbb{E}[V_t \mid W_{it}] = 0 \tag{8}$$

Centered and orthogonalized residuals are isolated from out-of-fold predictions to detect unexpected innovations strictly uncorrelated with the macroeconomic confounders:

$$\tilde{Y}_{i,t+h} = Y_{i,t+h} - \hat{g}_0^{h,-k}(W_{it}) \tag{9}$$

$$\tilde{D}_t = D_t - \hat{m}_0^{-k}(W_{it}) \tag{10}$$

4.3 Nonlinear tail-risk extension

Assuming linear macro-financial responses entails important limitations: an increase from one to two incidents is unlikely to generate the same marginal effect as an increase from eighteen to nineteen. High-intensity cyberattacks can overwhelm the shock-absorbing capacity of financial systems and trigger panic, whereas low-intensity events may fall below the threshold of market salience. To account for these nonlinearities, while following the Neyman orthogonality framework for heterogeneous treatment effects, I extend the baseline DML-LP framework by transforming the shock into a percentile-based tail risk threshold, denoted by D_t^{tail} in Equation (11):

$$\text{Extreme}_{it} = \mathbb{I}(D_{it} \geq \tau_{99}) \tag{11}$$

where $\mathbb{I}(\cdot)$ is an indicator function equaling 1 when the condition is satisfied, and 0 otherwise. To capture extreme tail-risk shocks that penetrate systemic financial infrastructure, I define τ_{99} as the 99th percentile of strictly positive cyber event counts across the panel. Setting this threshold at the extreme tails of the distribution aligns with established macro-finance literature on tail-risk events and financial vulnerability (Eichengreen et al., 2011).

The first-stage orthogonalization (Equations 7 through 10) follows the baseline setup, replacing the shock D_t with the binary tail-risk indicator D_t^{tail}. This allows the machine learning learners to isolate orthogonalized variation driven by severe network breaches from routine operational noise.

4.4 Second-stage DML-LP estimation

In the second stage, the dynamic impulse responses are identified by regressing the orthogonalized outcome residuals on the orthogonalized treatment residuals without an intercept, as specified in Equation (12):

$$\tilde{Y}_{i,t+h} = \beta^h \tilde{D}_t + \epsilon^h_{i,t+h} \tag{12}$$

Where β^h captures the causal macroeconomic impact of the systemic cyber shock at horizon h. For the nonlinear tail-risk extension, the continuous orthogonalized residual $\tilde{D}_t$ is simply substituted with the binary orthogonalized residual $\tilde{D}_t^{\text{tail}}$. The omission of a linear constant is methodologically required to prevent perfect multicollinearity, as the first-stage DML residuals are centered at an expected mean of zero by design.

The dynamic Impulse Response Function (IRF) is tracked across horizons by the parameter vector $\Phi = \{\beta^0, \ldots, \beta^5\}$. To rigorously account for intra-group correlation and heteroskedasticity, standard errors are estimated using robust sandwich covariance estimators clustered at the country level (Huber, 1967; White, 1980), as shown in Equation (13):

$$\text{Var}(\hat{\beta}^h) = (\mathbf{M}^T\mathbf{M})^{-1} \left(\sum_{c \in C} \mathbf{M}_c^T \hat{\epsilon}_c^h (\hat{\epsilon}_c^h)^T \mathbf{M}_c \right) (\mathbf{M}^T\mathbf{M})^{-1} \tag{13}$$

Where $\mathbf{M} = [\tilde{D}_t]$ is the second-stage regressor matrix of the orthogonalized treatment signal, and c indexes the country clusters.

5 Empirical Results

5.1 Baseline specification: The resilience of institutional buffers

To prevent spurious regressions, I first evaluate the integration properties of the panel variables using the Im-Pesaran-Shin (IPS) panel unit root test (Im et al., 2003). Table (3) reports these results, where optimal lag lengths are determined by the the Akaike Information Criterion (AIC) (Akaike, 2025) to balance model parsimony and goodness-of-fit.

Table 3: Im-Pesaran-Shin (IPS) Panel Unit Root Test Results

Variable	**IPS Statistic**	p**-value**	**Lags**	**Integration Order**
Panel A: Outcome and EMP Components				
Exchange Market Pressure (EMP)	-26.5248^{***}	0.0000	AIC	$I(0)$
Nominal Depreciation (% MoM, Δe)	-49.8521^{***}	0.0000	AIC	$I(0)$
Foreign Reserves Growth (% MoM, ΔR)	-40.4209^{***}	0.0000	AIC	$I(0)$
Policy Rate Change (pp, Δr)	-16.5435^{***}	0.0000	AIC	$I(0)$
Panel B: Cyber Shock and Macroeconomic Controls (W_{it})				
FMI Cyber Attacks (D)	-58.9937^{***}	0.0000	AIC	$I(0)$
Inflation Rate (% per annum, π)	-20.5765^{***}	0.0000	AIC	$I(0)$
Real GDP Growth Rate (% YoY, ΔGDP)	-9.2630^{***}	0.0000	AIC	$I(0)$
VIX CBOE (% MoM)	-18.0250^{***}	0.0000	AIC	$I(0)$
FED Funds Rate (% MoM)	-8.2232^{***}	0.0000	AIC	$I(1)$

Notes: Im-Pesaran-Shin (IPS) panel unit root test statistics across 30 emerging markets from 2015-2024. Lag selection is based on the Akaike Information Criterion (AIC). All test statistics reject the null hypothesis of a panel unit root at the 1% significance level ($^{***}p < 0.01$). Source: Author calculations.

Having confirmed the stationarity of the variables, I empirically test the propositions derived from the game-theoretical framework. I employ the Double Machine Learning Local Projections (DML-LP) approach to isolate the dynamic responses of exchange market pressure (EMP) to systemic financial market infrastructure cyber attacks (D) across 30 emerging markets. Figure (1) and Table (4) map the resulting impulse responses.

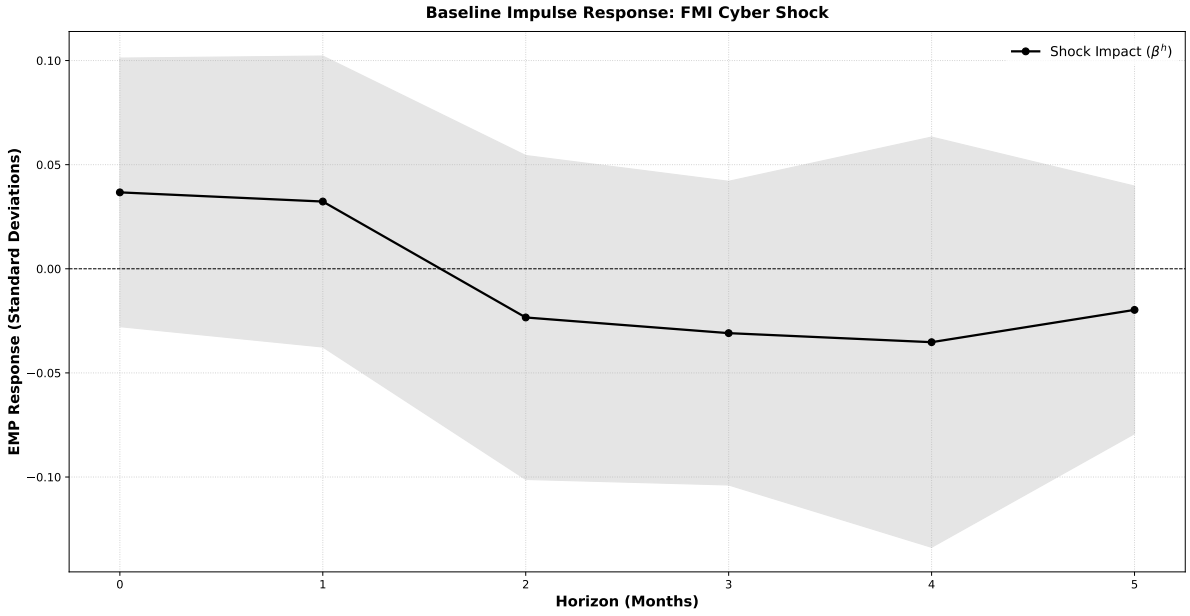


Figure 1: IRF of Exchange Market Pressure to a 1-SD FMI Cyber Attacks across Emerging Markets

Note: Local Projection impulse responses. Shaded areas illustrate 95% confidence intervals. The response is measured in standard deviations to a one-standard-deviation exogenous shock in systemic cyber attacks (1 SD corresponds to 1.868). Standard errors are clustered at the country level to account for autocorrelation and heteroskedasticity. The estimation contains country-specific historical time-means, pre-treatment lags, and seasonal fixed effects embedded within the first-stage Double Machine Learning nuisance architecture. Source: Author calculations

Table 4: Baseline IRF Estimates: EMP Response to a 1-SD FMI Cyber Attack

Dependent Variable	**Horizon 0**	**Horizon 1**	**Horizon 2**	**Horizon 3**	**Horizon 4**	**Horizon 5**
Exchange Market Pressure (EMP)	0.0367	0.0323	−0.0234	−0.0309	−0.0352	−0.0197
	(0.0329)	(0.0356)	(0.0397)	(0.0372)	(0.0503)	(0.0303)
Observations	N_0	N_1	N_2	N_3	N_4	N_5
Macro Controls			Yes			
Pre-treatment Lags			Yes			
Country Means (Mundlak)			Yes			
Season Fixed Effects			Yes			

Notes: Double Machine Learning Local Projections (DML-LP) estimates. The response is measured in standard deviations to a one-standard-deviation exogenous shock in global cyber attacks (1 SD refers to 1.868). Standard errors, clustered at the country level, are reported in parentheses directly below point estimates. Significance levels: $^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. The model includes pre-treatment lags, cross-sectional country means, and season fixed effect. Source: Author calculations.

Results under the baseline continuous specification demonstrate that routine, operational cyber attacks targeting financial market infrastructures (FMI) fail to generate significant Exchange Market Pressure (EMP). Across all horizons, a one-standard-deviation systemic cyber shock yields an EMP response that is statistically indistinguishable from zero. This empirical null result directly validates Proposition 1: institutional buffers smoothly absorb background operational noise that falls below the critical salience threshold.

This finding aligns with recent literature (Aldasoro et al., 2022; Smaga, 2025) demonstrating the resilience of central banks against moderate cyber risks and their capacity to utilize backup protocols to guarantee sufficient liquidity for domestic banking sectors. Crucially, under the CPMI-IOSCO international regulatory standards for cyber resilience (CPMI-IOSCO, 2016), systemically important clearing, settlement, and payment networks are mandated to meet a strict two-hour recovery time objective (2hRTO) to ensure the completion of final settlement by the end of the value date. Because trade settlements remain operational and critical financial networks remain intact, routine disruptions are successfully contained within these mandated intraday parameters. Consequently, low-to-moderate cyber attacks fail to trigger counterparty insolvency or structural liquidity freezes.

From a market participant perspective, foreign investors view routine technical disruptions as standard operational frictions rather than systemic threats capable of causing indefinite clearinghouse freezes. In accordance with the rational inattention framework (Sims, 2003), investors filter out this idiosyncratic operational noise and do not adjust their cross-border portfolio allocations based on minor infrastructural friction. Furthermore, as formalized by Abel et al. (2013), the presence of transaction and information costs creates broad inaction bands that deter investors from continuously monitoring or rebalancing their portfolios. The inherent covertness of cyber operations, combined with severe uncertainty regarding the true scale of standard FMI losses, generates significant information costs that strictly favor investor inaction. Thus, below the catastrophic threshold, global capital flows remain structurally undisturbed.

5.2 Nonlinearities of extreme tail-risk cyber attacks

I evaluate the impact of extreme FMI cyber attacks on exchange market pressure across emerging markets using DML-LP framework. Figure (2) and (5) map the impulse responses:

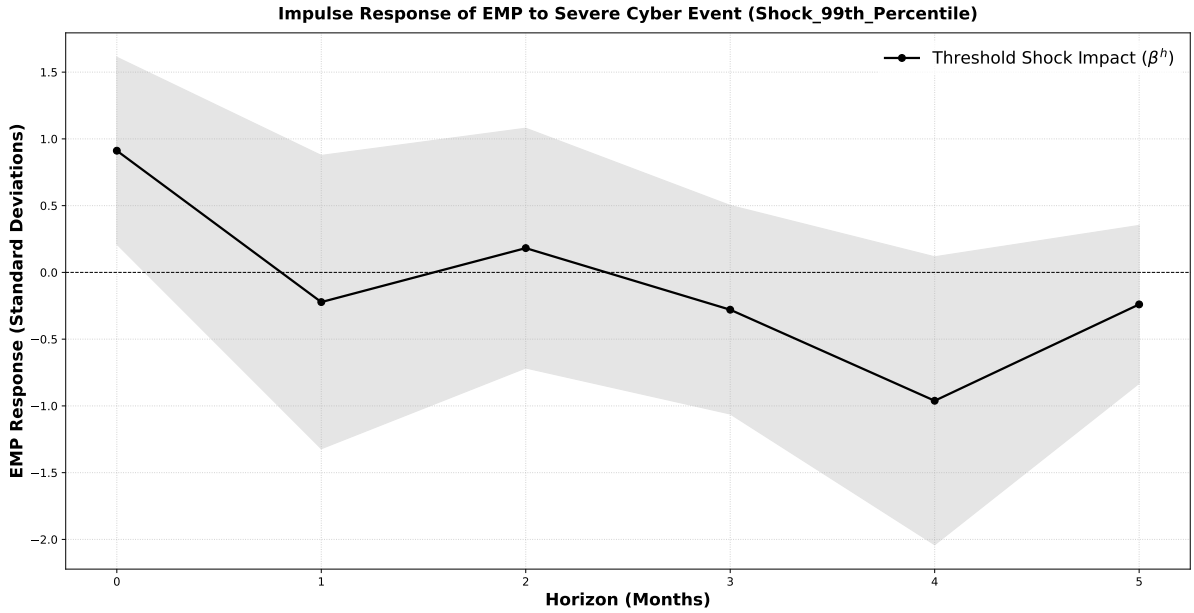


Figure 2: Nonlinear IRF of EMP to Extreme Tail-Risk FMI Cyber Shocks (99th Percentile)

Note: Local Projection impulse responses. Shaded areas illustrate 95% confidence intervals. The response is measured in standard deviations to a one-standard-deviation in systemic FMI cyber attacks. Standard errors are clustered at the country level to account for autocorrelation and heteroskedasticity. The estimation containes country-specific historical time-means, pre-treatment lags, and season fixed effects embedded within the first-stage Double Machine Learning nuisance architecture. Source: Author calculations.

Table 5: Nonlinear IRF Estimates: EMP Response to an Extreme Tail Cyber Shock (99th Percentile)

Dependent Variable	**Horizon 0**	**Horizon 1**	**Horizon 2**	**Horizon 3**	**Horizon 4**	**Horizon 5**
Exchange Market Pressure (EMP)	0.9115^{**}	-0.2224	0.1819	-0.2796	-0.9615^{*}	-0.2397
	(0.3571)	(0.5605)	(0.4581)	(0.3985)	(0.5502)	(0.3018)
Observations	N_0	N_1	N_2	N_3	N_4	N_5
Macro Controls			Yes			
Pre-treatment Lags			Yes			
Country Means (Mundlak)			Yes			
Season Fixed Effects			Yes			

Notes: Double Machine Learning Local Projections (DML-LP) estimates. The treatment corresponds to a binary tail-risk cyber shock defined at the 99th percentile (D_t^{tail}). Standard errors, clustered at the country level, are reported in parentheses directly below point estimates. Significance levels: $^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. The model includes pre-treatment lags, cross-sectional country means, and season fixed effect. Source: Author calculations.

Results indicate that breaching the extreme tail-risk threshold (99th percentile) of systemic cyber attacks targeting financial market infrastructures generates a statistically significant, immediate surge in exchange market pressure of 0.9115^{**} standard deviations. This finding empirically validates the informational opacity and strategic run dynamics outlined in Proposition 2 ($\beta_{\text{EMP}} > 0$). Considering that standard international finance literature traditionally defines a localized speculative currency crisis as an EMP surge

of at least two standard deviations (Eichengreen et al., 1994), an extreme cyber campaign alone accounts for nearly half of this threshold simultaneously across 30 emerging markets. Because this 0.9115** standard deviation surge represents an average cross-sectional response rather than an isolated country, it establishes the premise of a synchronized, widespread currency crisis across the emerging market periphery, severely exacerbating existing macro-financial vulnerabilities.

Existing literature predominantly focuses on how cyber shocks destabilize micro-level banking firms (Eisenbach et al., 2022; Pollmeier et al., 2023; Gaies et al., 2026), leaving significant ambiguity regarding how these technological shocks propagate at the macroeconomic level. These results demonstrate that extreme cyber attacks targeting critical financial market infrastructures directly interact with aggregate capital flows to generate severe exchange market pressure. This immediate surge reflects a deep institutional vulnerability to highly coordinated, state-sponsored campaigns targeting the central clearing nodes of global finance. This finding corroborates broader assessments by international financial institutions and central banks on the systemic nature of cyber threats (Kopp et al., 2017; Adelmann et al., 2020; Doerr et al., 2022), confirming the premise that network interconnectedness serves as a primary transmission channel for cross-border liquidity retrenchment (IMF, 2024a; OECD, 2026).

The canonical first through third generations of currency crisis models (Krugman, 1979; Obstfeld, 1984; Eichengreen et al., 1994) focus primarily on sovereign insolvency, balance sheet mismatches, or self-fulfilling macroeconomic speculative attacks. The findings presented here introduce a distinct, technologically driven channel. They demonstrate that the self-fulfilling panic dynamics modeled by Obstfeld (1996) and Bernardo and Welch (2004) are triggered when the informational opacity of extreme cyberattacks intersects with operational paralysis across financial market infrastructures. Fearing a systemic liquidity freeze and trapped capital within settlement bottlenecks, investors rush to exit high-beta peripheral assets.

A potential econometric concern is that the aggregate EMP response could be artificially driven by domestic monetary policy tightening, creating the illusion of a flight-to-safety shock. Because the composite index internalizes policy interest rates, an aggressive central bank rate hike could mathematically mimic a currency stress. To demonstrate that the observed tail-risk EMP spike is driven by genuine cross-border capital flight rather than confounding domestic rate interventions, the composite index is completely disaggregated. The DML-LP framework is re-estimated for each individual component independently to isolate the exact transmission channel. The results are presented in Table 6:

Table 6: Mechanism Verification: Disaggregating EMP at the Extreme Threshold

Dependent Variable	**Horizon 0**	**Horizon 1**	**Horizon 2**	**Horizon 3**	**Horizon 4**	**Horizon 5**
Panel A: Nominal Exchange Rate Depreciation (Δe)						
Tail-Risk Cyber Shock	1.5238^{***}	-0.9825	-0.3784	-1.1765	-1.3742^{*}	0.2730
	(0.4153)	(0.7056)	(0.7870)	(0.7781)	(0.7019)	(0.4555)
Observations	3,454	3,429	3,404	3,377	3,350	3,322
Panel B: Reserve Depletion (ΔR)						
Tail-Risk Cyber Shock	-1.6007	-0.9383	1.8633	1.3160	11.7272^{*}	-5.1280
	(2.0096)	(3.1523)	(3.2180)	(2.7751)	(6.8673)	(4.1635)
Observations	3,256	3,226	3,202	3,174	3,146	3,118
Panel C: Policy Interest Rate Differentials (Δr)						
Tail-Risk Cyber Shock	-0.0443	0.0083	0.0460	-0.3622	0.0315	-0.1460
	(0.2425)	(0.2707)	(0.1852)	(0.3986)	(0.3322)	(0.2921)
Observations	3,449	3,423	3,398	3,371	3,344	3,316
Pre-treatment Lags			Yes			
Correlated Random Effects			Yes			
Season Fixed Effects			Yes			
Cluster at country level			Yes			

Notes: The table disaggregates the composite EMP index into its foundational components using the DML-LP framework. The shock is a binary indicator for catastrophic global cyber attacks (99th percentile, $D_t \geq 10$). Standard errors, clustered at the country level, are reported in parentheses. Significance levels: $^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. The model includes pre-treatment lags, cross-sectional country means, and seasonal fixed effects. Source: Author calculations.

Under extreme tail-risk cyber shocks, the component-level estimates provide robust empirical support for Proposition 3, confirming the core-periphery flight-to-safety mechanism. Crucially, the interest rate response (Δr) across all horizons is economically negligible and statistically indistinguishable from zero. Conversely, the exchange rate component exhibits a massive, highly significant positive response on impact ($\beta_{\Delta e_{it}} = 1.5238, p < 0.01$), indicating a sharp nominal depreciation. Because central banks neither systematically hike rates nor execute sufficiently aggressive reserve interventions to arrest the depreciation, the pressure is entirely absorbed by the collapse of the currency value. This divergence confirms that domestic monetary policy tightening is not artificially driving the observed surge in aggregate exchange market pressure. Rather, the EMP spike reflects genuine, exogenous capital flight as investors abandon emerging market exposure for the safety of the US dollar.

Traditional asset pricing literature posits that distressed investors overwhelmingly seek refuge in lower-volatility, highly liquid assets during macroeconomic crises (Sarwar, 2017; Adrian et al., 2019). These findings expand this paradigm by demonstrating a severe geographic asymmetry in systemic technological shocks. Even when the targeted financial market infrastructures (e.g., SWIFT, Fedwire, DTCC) are physically centralized in advanced core economies, foreign investors reflexively liquidate periphery assets to hoard core-market safe havens. This asymmetric contagion structurally exacerbates the financial fragmentation of emerging markets from the global financial system.

While the profound structural interconnectedness and systemic choke points of the global financial system leave core infrastructure inherently vulnerable to operational breaches, frontier advancements in artificial intelligence and adversarial offensive tools can disproportionately favor attackers (Aldasoro et al., 2026; Adrian et al., 2019). As the frequency of state-sponsored cyber warfare continues to escalate (IMF, 2024a; Singh, 2025), this dynamic constitutes a profound, rising threat to global macro-financial stability. Rogue geopolitical actors and heavily sanctioned states increasingly deploy systemic cyber operations to extract hard currency and bypass international embargoes.

Regardless of whether the attacker's primary motive is direct financial theft or strategic geoeconomic sabotage, the extreme escalation of these operations severely damages the credibility and operational resilience of global financial plumbing. Consequently, emerging markets are structurally forced to absorb the macroeconomic fallout through intense currency pressure. Ultimately, the convergence of heightened geopolitical tensions and advanced, AI-driven cyber threats targeting global payment systems fosters a systemic contagion that accelerates global financial fragmentation, decisively reversing decades of presumed macro-financial integration.

5.3 Robustness checks: placebo falsification tests

To confirm the baseline DML-LP causal identification, I conduct a non-parametric permutation test, as illustrated in Figure (3). By randomizing the chronological timeline of the systemic FMI cyber attacks and re-estimating the regime-dependent impulse response functions across 100 independent iterations, I construct the true empirical null distribution of the treatment effect.

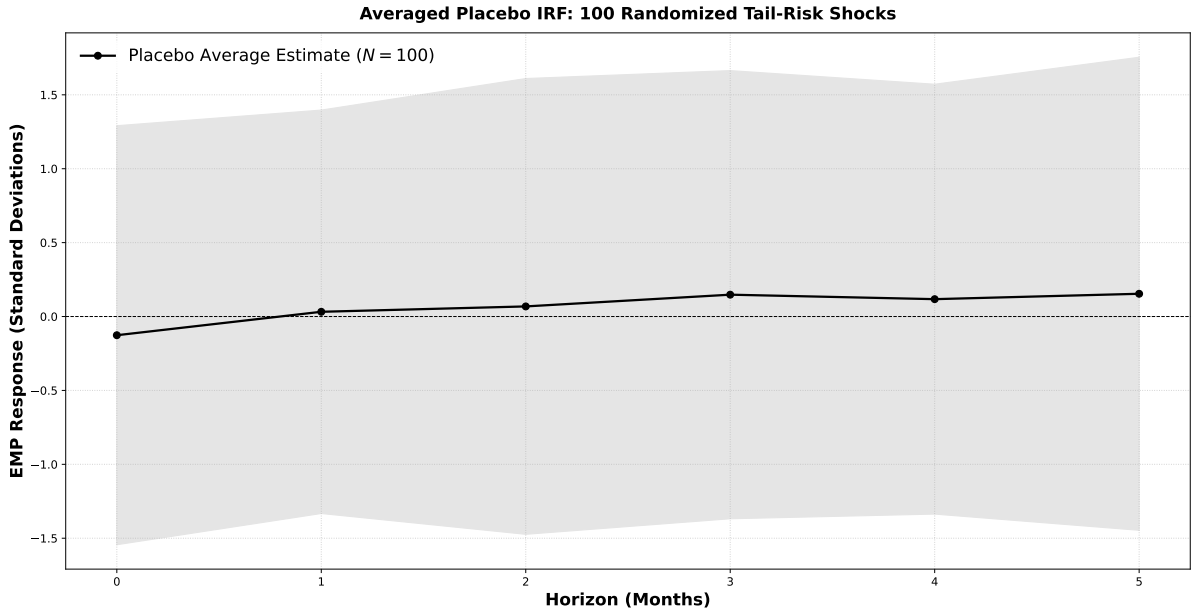


Figure 3: Averaged Placebo IRF: 100 Randomized Cyber Attack Permutations

Note: Double Machine Learning Local Projections (DML-LP) estimates. Shaded areas illustrate 95% confidence intervals. The response is measured in standard deviations to a one-standard-deviation shock in FMI cyber attacks. Standard errors are clustered at the country level to account for autocorrelation and heteroskedasticity. The estimation utilizes country-specific historical time-means, pre-treatment lags, and season fixed effects embedded within the first-stage DML nuisance architecture. Source: Author calculations

Across all horizons, the averaged placebo estimates yield coefficients that are statistically indistinguishable from zero. The widened confidence intervals confirm that randomizing the shock sequence degrades the structural signal into pure statistical noise. This falsification procedure robustly confirms that the baseline exchange market pressure dynamics are causally driven by the actual timing of cyber attacks, rather than spurious confounding dynamics.

6 Conclusion

In an era of hyper-interconnected digital financial infrastructure, the weaponization of systemic cyber operations has introduced a critical new transmission channel for currency pressure and geoeconomic fragmentation. By inducing severe informational opacity and operational paralysis, these technological shocks exploit the structural vulnerabilities of global financial market infrastructures, fundamentally altering the coordinated behavior of foreign investors.

The empirical findings presented in this paper demonstrate a stark, nonlinear macro-financial vulnerability. While low-to-moderate cyber disruptions are smoothly absorbed by existing institutional buffers and

mandated intraday recovery protocols, extreme tail-risk cyber attacks weaken this resilience. At the 99th percentile of severity, systemic cyber shocks trigger an immediate, highly significant surge in exchange market pressure across the emerging market periphery. As foreign investors instinctively liquidate emerging market exposure to hoard core-market safe havens, emerging economies are forced to absorb the macroeconomic fallout, severely exacerbating existing financial vulnerabilities and fragmentation.

While this paper isolates and measures the macroeconomic impact of historical cyber incidents that actively targeted financial networks, the escalating sophistication of state-sponsored actors heightens the threat of unprecedented future disruptions. Incorporating targeted cyber-shock scenarios focused on clearing and settlement infrastructure into standard sovereign debt and asset-pricing models represents an essential and natural progression for the macro-finance literature.

Data Availability Statement

Replication data and code are available upon request and will be made publicly accessible via an open-source repository upon publication.

References

Abel, A. B., J. C. Eberly, and S. Panageas (2013). Optimal inattention to the stock market with information costs and transactions costs. *Econometrica 81*(4), 1455–1481.

Adelmann, F., I. Ergen, T. Gaidosch, N. Jenkinson, M. T. Khiaonarong, A. Morozova, N. Schwarz, and C. Wilson (2020). *Cyber risk and financial stability: It'sa small world after all.* International Monetary Fund.

Adrian, T., R. K. Crump, and E. Vogt (2019). Nonlinearity and flight-to-safety in the risk-return trade-off for stocks and bonds. *The Journal of Finance 74*(4), 1931–1973.

Akaike, H. (2025). Akaike's information criterion. In *International encyclopedia of statistical science*, pp. 41–42. Springer.

Aldasoro, I., R. Auer, J. Frost, and F. Perez-Cruz (2026). A mythos moment? frontier ai and cyber risk. Technical report, Bank for International Settlements.

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach (2022). The drivers of cyber risk. *Journal of financial stability 60*, 100989.

Auerbach, A. J. and Y. Gorodnichenko (2012). Measuring the output responses to fiscal policy. *American Economic Journal: Economic Policy 4*(2), 1–27.

Bernardo, A. E. and I. Welch (2004). Liquidity and financial market runs. *The Quarterly Journal of Economics 119*(1), 135–158.

BIS (2024). Central bank policy rates database (cbpol). Accessed: 2026-07-25.

Board of Governors of the Federal Reserve System (US) (2024). Federal Funds Effective Rate [FEDFUNDS]. Federal Reserve Bank of St. Louis (FRED). Accessed: 2024-12-31.

Breiman, L. (2001). Random forests. *Machine learning 45*(1), 5–32.

Caporale, G. M., W.-Y. Kang, F. Spagnolo, and N. Spagnolo (2020). Non-linearities, cyber attacks and cryptocurrencies. *Finance Research Letters 32*, 101297.

Chernozhukov, V., D. Chetverikov, M. Demirer, E. Duflo, C. Hansen, W. Newey, and J. Robins (2018). Double/debiased machine learning for treatment and structural parameters.

Chiboub, I. and H. Sadok (2026). Weaponizing climate policy: Carbon tariffs, retaliatory threats, and exchange rate regimes. *Available at SSRN 7037458*.

Chicago Board Options Exchange (2024). CBOE Volatility Index: VIX [VIXCLS]. Federal Reserve Bank of St. Louis (FRED). Accessed: 2024-12-31.

CPMI-IOSCO (2016, June). Guidance on cyber resilience for financial market infrastructures. Policy Report CPMI Papers No. 146, Committee on Payments and Market Infrastructures and International Organization of Securities Commissions.

Crespo, R. A. (2018). Currency warfare and cyber warfare: The emerging currency battlefield of the 21st century. *Comparative Strategy 37*(3), 235–250.

Doerr, S., L. Gambacorta, T. Leach, B. Legros, and D. Whyte (2022). *Cyber risk in central banking*. Bank for International Settlements, Monetary and Economic Department.

Eichengreen, B., R. Gullapalli, and U. Panizza (2011). Capital account liberalization, financial development and industry growth: A synthetic view. *Journal of International Money and Finance 30*(6), 1090–1106.

Eichengreen, B., A. K. Rose, and C. Wyplosz (1994). Speculative attacks on pegged exchange rates: an empirical exploration with special reference to the european monetary system.

Eisenbach, T. M., A. Kovner, and M. J. Lee (2022). Cyber risk and the us financial system: A pre-mortem analysis. *Journal of Financial Economics 145*(3), 802–826.

Finkle, J. and J. Wagstaff (2016, May). Special report: Cyber thieves exploit banking network's weak links. *Reuters*. Accessed: 2026-09-05.

Frankel, D. M., S. Morris, and A. Pauzner (2003). Equilibrium selection in global games with strategic complementarities. *Journal of Economic Theory 108*(1), 1–44.

Gaies, B., N. Chaâbane, and J.-M. Sahut (2026). Cyber risk, market fear and financial instability: hunting down risk through contagion analysis. *Journal of Economic Studies 53*(5), 1012–1032.

Girton, L. and D. Roper (1977). A monetary model of exchange market pressure applied to the postwar canadian experience. *The American economic review 67*(4), 537–548.

Ha, J., M. A. Kose, and F. Ohnsorge (2023, October). One-stop source: A global database of inflation. *Journal of International Money and Finance 137*, 102896.

Harry, C. and N. Gallagher (2018). Classifying cyber events. *Journal of Information Warfare 17*(3), 17–31.

Huber, P. J. (1967). The behavior of maximum likelihood estimates under nonstandard conditions. In *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability*, Volume 1, Berkeley, CA, pp. 221–233. University of California Press.

Im, K. S., M. H. Pesaran, and Y. Shin (2003). Testing for unit roots in heterogeneous panels. *Journal of econometrics 115*(1), 53–74.

IMF (2024a, April). Cyber risk: A growing concern for macrofinancial stability. In *Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks*, Chapter 3, pp. 77–102. Washington, DC: International Monetary Fund.

IMF (2024b). International reserves and foreign currency liquidity (irfcl) dataset. Accessed: 2026-07-25.

IMF (2024c). Quarterly national accounts (qnea) dataset. Accessed: 2026-07-25.

IMF (2025). Annual report on exchange arrangements and exchange restrictions. Accessed: 2026 07 28.

ITC (2015). Global cybersecurity index 2015. Technical report, International Telecommunication Union (ITU), Geneva, Switzerland.

ITC (2018). Global cybersecurity index 2018. Technical report, International Telecommunication Union (ITU), Geneva, Switzerland.

ITC (2021). Global cybersecurity index 2021. Technical report, International Telecommunication Union (ITU), Geneva, Switzerland.

ITC (2024). Global cybersecurity index 2024. Technical report, International Telecommunication Union (ITU), Geneva, Switzerland.

Jordà, Ò. (2005). Estimation and inference of impulse responses by local projections. *American economic review 95*(1), 161–182.

Khiaonarong, T. and S. Zheng (2026). The rise of cyber events and digital fraud in the financial sector.

Kopp, E., L. Kaffenberger, and N. Jenkinson (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Krugman, P. (1979). A model of balance-of-payments crises. *Journal of money, credit and banking 11*(3), 311–325.

Maurer, T. and A. Nelson (2021, March). The global cyber threat to financial systems. *Finance & Development*. Accessed: 2026-09-05.

Morris, S. and H. S. Shin (1998). Unique equilibrium in a model of self-fulfilling currency attacks. *American Economic Review 88*(3), 587–597.

Mundlak, Y. (1978). Models with variable coefficients: Integration and extension. In *Annales de l'INSEE*, pp. 483–509. JSTOR.

Obstfeld, M. (1984). Rational and self-fulfilling balance-of-payments crises. Technical report, National Bureau of Economic Research.

Obstfeld, M. (1996). Models of currency crises with self-fulfilling features. *European economic review 40*(3-5), 1037–1047.

OECD (2026). Cybersecurity and geopolitical risks in financial markets. OECD Business and Finance Policy Papers 104, Organisation for Economic Co-operation and Development, Paris.

Pollmeier, S., I. Bongiovanni, and S. Slapničar (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science 159*, 106022.

Ramey, V. A. and S. Zubairy (2018). Government spending multipliers in good times and in bad: evidence from us historical data. *Journal of political economy 126*(2), 850–901.

Reuters Editorial (2016, May). Vietnam bank says thwarted swift messaging fraud attempt. *Reuters*. Accessed: 2026-09-05.

Rey, H. (2015). Dilemma not trilemma: the global financial cycle and monetary policy independence. Technical report, National Bureau of Economic Research.

Sarwar, G. (2017). Examining the flight-to-safety with the implied volatilities. *Finance Research Letters 20*, 118–124.

Sims, C. A. (2003). Implications of rational inattention. *Journal of monetary Economics 50*(3), 665–690.

Singh, T. (2025). Case studies: state-sponsored cyberattacks. In *Cybersecurity, Psychology and People Hacking*, pp. 151–165. Springer.

Smaga, P. (2025). Evaluating cyber attacks on central banks–identification of trends in cyber threat landscape. *Computers & Security*, 104742.

Tian, S., B. Zhao, and R. O. Olivares (2023). Cybersecurity risks and central banks' sentiment on central bank digital currency: Evidence from global cyberattacks. *Finance Research Letters 53*, 103609.

White, H. (1980). A heteroskedasticity-consistent covariance matrix estimator and a direct test for heteroskedasticity. *Econometrica 48*(4), 817–838.

Yahoo Finance (2025). Exchange rate data. Accessed: 2026-07-25.

A Online Appendix

A.1 Data Details

Table 7: Variable Definitions and Data Sources

Variable	Description	Freq.	Source
Panel A: Main Empirical Variables			
EMP_{it}	Exchange Market Pressure index, calculated as the variance-weighted sum of nominal depreciation, reserve depletion, and policy rate hikes.	Monthly	Author calculations
D_t	Systemic Cyber Shock index, counting disruptive incidents targeting critical global financial market infrastructure (FMI).	Monthly	UMD CISSM
Panel B: Underlying EMP Components			
Δe_{it}	Nominal depreciation, measured as the month-over-month percentage change in national currency per USD.	Monthly	Yahoo Finance
ΔR_{it}	Foreign exchange reserve growth, measured as the month-over-month percentage change in total reserves.	Monthly	IMF IRFCL
Δr_{it}	Policy rate change, measured as the month-over-month difference in central bank interest rates (in percentage points).	Monthly	BIS
Panel C: Macroeconomic and Institutional Controls			
Inflation Rate	Year-over-year percentage change in the consumer price index.	Monthly	Ha et al. (2023)
Real GDP Growth	Year-over-year percentage change in real GDP (forward-filled step-wise to match the monthly panel).	Quarterly	IMF QNEA
Exchange Rate Regime	Binary indicator equal to 1 for floating regimes and 0 for pegged/fixed arrangements, based on dynamic de facto classifications.	Monthly	IMF
Cybersecurity Index ($\overline{GCI}_i$)	Country-specific time-invariant baseline of institutional cybersecurity capacity, derived from historical mean scores.	Triennial	ITU

Notes: This table outlines the definitions, raw reporting frequencies, and institutional sources for the variables utilized in the 2015 to 2024 emerging market panel. Variables reported at lower frequencies (e.g., quarterly GDP, triennial GCI) are transformed as specified in Section 3 to maintain the continuous monthly estimation framework without introducing look-ahead bias.