Systemic Cyber Attacks, Informational Opacity, and Exchange Market Pressure in Emerging Markets

Ilias Chiboub*

Abstract

Systemic cyber shocks introduce a novel transmission channel for currency runs and financial contagion. To capture the strategic drivers of this exchange market pressure, I model a dynamic game of incomplete information among a state-sponsored attacker, a central bank defender, and foreign investors. I empirically test the resulting propositions using a Double Machine Learning Local Projections framework on a panel of 30 emerging markets from 2015 to 2024. Results demonstrate that cyber attacks trigger speculative currency attacks under fixed regimes, where foreign investors operate at a severe informational disadvantage regarding operational losses and reserve adequacy. In contrast, continuous price discovery under floating regimes rapidly internalizes shocks and reflects underlying market positions, leading to an immediate dissipation of exchange market pressure. During severe cyber attacks, this transparency activates a flight-to-safety reallocation, driving capital away from the opaque vulnerabilities of pegged regimes toward the shock-absorbing float. Ultimately, these findings establish that exchange rate regimes fundamentally dictate the pricing of systemic cyber shocks, revealing that foreign investors favor transparent price discovery over artificially suppressed nominal volatility.

Keywords: Cyber risk, Exchange rate regime, Speculative attacks, Game theory, Causal Machine Learning, Emerging markets

JEL Classification: F31, F32, G15, C73, 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 financial stability, capable of triggering severe financial contagion (Kopp et al., 2017; Adelmann et al., 2020; Doerr et al., 2022). Systemic, high-velocity cyber incidents can halt payment settlement and interbank clearing networks. In the resulting opacity, market participants often misattribute these sudden non-payments to fundamental insolvency, triggering liquidity hoarding and credit freezes (IMF, 2024a; OECD, 2026). The interconnected architecture of global finance relies on critical chokepoints, such as SWIFT, CLS Bank, and Fedwire; consequently, an attack targeting a single node forces these networks to delay settlement chains or temporarily sever connections. These settlement failures can quickly evolve into diminished market confidence and exchange market pressure, sparking broader fragmentation. Even in the absence of targeted domestic attacks, shocks to these global networks can abruptly sever an economy's foreign exchange capacity, precipitating rapid cross-border contagion. For central banks, these incidents are no longer viewed as isolated IT failures, but rather as systemic risks associated with massive financial 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 these shocks interact with aggregate capital flows and exchange rate markets 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 deploy sophisticated zero-day exploits and distributed denial-of-service operations to covertly disrupt critical payment architectures over extended horizons (Singh, 2025), converting transitory operational disturbances into structural macro-financial shocks. Under this cyber-induced distress, foreign investors face severe loss uncertainty, which amplifies risk aversion and triggers sudden capital flight. Because capital drain exerts intense pressure on the currency, the exchange rate regime determines how the shock is absorbed, introducing a structural trade-off between continuous price discovery and nominal anchoring. I therefore investigate a central question for financial stability: how do systemic financial cyber attacks transmit into exchange market pressure across different currency regimes?

This question carries substantial implications for foreign investors, financial institutions, central banks, and sovereign authorities, particularly across emerging markets operating under heterogeneous exchange rate regimes. These agents face fundamental uncertainty because, under covert and high-velocity cyber attacks, verifying account balances and liquidity solvency requires time-intensive forensic audits, which fragments the market's knowledge base and obscures data. Floating regimes facilitate continuous real-time price dis-

covery that allows foreign investors to evaluate the realized magnitude of a shock against a transparent benchmark. Furthermore, consistent with the established macroeconomic literature, this flexibility provides a greater absorption capacity for external disturbances through immediate exchange rate adjustments (Edwards and Yeyati, 2005). In contrast, pegged regimes insulate nominal exchange rates from immediate volatility (Kočenda and Valachy, 2006), but do so by generating severe information asymmetries regarding losses and true reserve adequacy. Informational opacity structurally fosters speculative attacks and self-fulfilling currency runs, as foreign investors seek to exit before central bank reserves are fully exhausted (Obstfeld, 1984, 1996). I demonstrate that systemic global financial cyber shocks act as a novel, exogenous trigger for this contagion mechanism. Modern finance relies on a few highly centralized institutional chokepoints and retail banks do not operate in a vacuum; they rely on correspondent banking networks to settle cross-border payments. Fearing counterparty risk, foreign banks immediately freeze credit lines to all banks in that affected country to protect themselves. This turns a localized operational shock into a cross-border interbank liquidity squeeze (Zoricakova et al., 2026). This structural interconnectedness acts as a severe amplifier, generating massive cross-border spillover risks from systemic cyber shocks (OECD, 2026).

To formalize these dynamics, I develop a dynamic game of incomplete information and adaptive learning (Morris and Shin, 1998; Evans and Honkapohja, 2001) among three strategic players: a foreign state-sponsored attacker, a central bank defender, and 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 of systemic global financial 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 navigate these challenges and perform robust causal identification, I employ a state-dependent Double Machine Learning Local Projections (DML-LP) framework (Jordà, 2005; Chernozhukov et al., 2018) with double residualization.

Consequently, the analysis establishes three core transmission mechanisms:

- **Peg Vulnerability and Self-fulfilling Prophecies:** Under fixed regimes, foreign investors operate at a severe informational disadvantage. Because nominal exchange rate movements are artificially suppressed, uncertainty regarding potential losses and peg sustainability escalates acutely, generating significant exchange market pressure through speculative currency attacks and preemptive capital flight.

- **Float Absorption and Transparent Price Discovery:** Under a floating regime, continuous price discovery provides a transparent benchmark that internalizes shocks and reflects underlying market

positions. This mechanism results in the immediate dissipation of market pressure, even during severe cyber attacks, effectively neutralizing the geoeconomic gain for the attacker.

- **The Flight-to-Safety Mechanism:** The resilience of floating regimes actively triggers a flight-to-safety reallocation. During systemic cyber events, foreign investors dynamically shift capital away from the opaque vulnerabilities of pegged regimes and toward the transparent shock-absorption of floating currencies.

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 literature on cyber risk in global finance. While existing macroeconomic 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 and central bank digital currencies (CBDC) (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 incidents as macroeconomic shocks transmitting directly into exchange market pressure. This aligns with recent evidence demonstrating that operational cyber losses can escalate into severe macroprudential concerns (Boungou, 2023; Kotidis and Schreft, 2025).

Second, I contribute to the foundational literature on exchange rate regimes, speculative attacks, and currency crises (Eichengreen et al., 1994; Obstfeld, 1996; Edwards and Yeyati, 2005). I show that the traditional shock-absorbing properties of floating regimes remain resilient even under severe cyber tail risks. Furthermore, I demonstrate that the mechanics of currency runs under fixed regimes can be triggered entirely by cyber-induced informational opacity and loss uncertainty, independent of classic macroeconomic misalignments. While first- through third-generation currency crisis models focus primarily on sovereign insolvency or self-fulfilling capital flight, my framework introduces systemic geoeconomic shocks as a novel, independent trigger for speculative attacks and exchange market pressure.

Third, I add a critical nuance to the literature regarding the flight-to-safety mechanism (Adrian et al., 2019; Sarwar, 2017). I demonstrate that during periods of extreme uncertainty, forward-looking investors favor transparent price discovery with higher baseline nominal volatility over artificially suppressed nominal volatility plagued by acute informational opacity. By estimating a four-state nonlinear model, I demonstrate that the transmission of these shocks is highly asymmetric, as severe cyber incidents disproportionately drive capital flight and trigger a flight to safety.

Fourth, I advance the empirical literature on state-dependent 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 and untested theoretical assumptions, I deploy a highly flexible, state-dependent DML-LP framework (Jordà, 2005; Chernozhukov et al., 2018). I embed a Hybrid-Mundlak transformation (Mundlak, 1978) directly into the machine learning first-stage nuisance equations to rigorously handle unobserved country-level heterogeneity within this nonlinear setting. By applying this advanced semi-parametric approach to the cyber domain, the model effectively isolates the nonlinear asymmetries inherent in shock propagation across baseline, fragile, and defensive states, while mitigating high-dimensional regularization bias.

Understanding this cyber risk transmission channel carries profound implications for international macro-finance, asset pricing, and systemic financial risk. Specifically, the empirical findings demonstrate that cyber attacks act as systemic, regime-dependent macroeconomic shocks rather than isolated micro-level operational hazards. Furthermore, these dynamics reveal a novel geoeconomic reality: the structural rigidities of a fixed exchange rate inadvertently weaponize informational opacity. State-sponsored attackers can strategically exploit these constraints to trigger self-fulfilling speculative attacks and financial contagion, exposing sovereign foreign exchange reserves to cyber-induced attrition. In contrast, floating currencies fundamentally deter such attacks by neutralizing the geoeconomic gain through continuous, transparent price discovery.

The remainder of the paper is organized as follows: In Section (2), I model the theoretical framework and solve the dynamic game of incomplete information. In Section (3), I introduce the data and summary statistics. In Section (4), I present the DML-LP empirical strategy. In Section (5), I discuss the empirical results. Finally, in Section (6), I conclude.

2 The Game Theory Model

2.1 Game structure and players

I model a dynamic game of incomplete information and adaptive learning (Morris and Shin, 1998; Evans and Honkapohja, 2001) in which a foreign state-sponsored attacker uses cyber attacks to provoke financial instability in a target economy, forcing the foreign exchange rate market to assimilate the operational shock. This game-theoretic approach is essential for formally capturing strategic incentives, information asymmetries, Bayesian belief formation, and complex payoff structures.

An incomplete information framework is critical in this environment. Unlike standard repeated games that sustain equilibrium through observable histories and retaliation threats, state-sponsored cyber attacks operate covertly. Furthermore, the distinct dynamics of exchange rate regimes conceal true market liquidity,

central bank intervention capacity, and the ultimate severity of the shock. This environment generates severe uncertainty and complex belief formation regarding player payoffs.

I assign three players that execute sequential decisions in each time period ($t = 1, 2, \dots$):

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

  Action: Chooses the intensity of the cyber attack shock $D_t \in [0, \bar{D}]$

  Payoff: Maximizes a utility function U_{FA} in Equation (1):

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

  Where θ refers to the geoeconomic gain for inducing exchange market pressure (EMP formally defined in Equation 4 below) and $c(D_t)$ capture the economic costs and attribution risks associated with launching the cyber attack.

- **Player 2 (Central Bank Defender):**

  Action: Sets an exchange rate policy commitment $j \in \{\text{fixed}, \text{float}\}$ and a corresponding, potentially unobservable, market intervention level.

  Payoff: Adapting the loss function of standard second-generation currency crisis models (Obstfeld, 1984, 1996), the central bank maximizes $U_{CB}(j)$ in Equation (2), intervening to minimize exchange market volatility subject to the macro-financial costs (C) of depleting reserves (R) or hiking rates (r), where $\alpha > 0$ represents the sensitivity to financial stability costs.

$$U_{CB}(j) = -\mathbb{E}[EMP_t^2] - \alpha \cdot C(R_t, r_t) \tag{2}$$

- **Player 3 (Foreign Investors):**

  Action: Observe the realized signal of the cyber attack ($\mathcal{S}_t$) and the exchange rate regime (j) to execute a portfolio allocation $\kappa_t \in \{\text{Hold}, \text{Run}\}$.

  Payoff: Following the standard portfolio choice theory, foreign investors maximize a mean-variance utility function $U_{FI}(\kappa_t)$ in Equation (3), optimizing their expected portfolio returns (π_t) while discounting devaluation risk based on their information set ($\mathcal{H}_t$).

$$U_{FI}(\kappa_t) = \mathbb{E}[\pi_t \mid \mathcal{H}_t] - \frac{\gamma}{2}\text{Var}(\pi_t \mid \mathcal{H}_t) \tag{3}$$

2.2 Timing and information asymmetry

The flow of information and signal observation depends strictly on the central bank's policy commitment, generating two distinct information sets ($\mathcal{H}_t$):

- **Under a fixed regime (Delayed Feedback):** $\mathcal{H}_t^{\text{Peg}} = \{a_0, a_1, \ldots, a_{t-L}\}$

  Information is delayed by an unknown lag L. The attacker launches a cyber attack at time t but cannot observe its true impact on central bank reserve adequacy until period $t + L$. Simultaneously, the central bank intervenes to stabilize the parity but struggles to distinguish an isolated cyber incident from a systemic, state-sponsored offensive campaign. Foreign investors allocate capital blindly based on beliefs, as true reserve depletion remains unobservable until official reporting at time $t + L$, leaving peg sustainability uncertain.

- **Under a floating regime (Instant Feedback):** $\mathcal{H}_t^{\text{Float}} = \{a_0, a_1, \ldots, a_t, e_t\}$

  Nominal fluctuations in the spot exchange rate (e_t) serve as an immediate price discovery mechanism. The flexibility of the exchange rate reveals the severity of the shock and capital flow shifts to all players in real time. The central bank makes no commitment to defend a parity, neutralizing the information asymmetry regarding reserve solvency. Foreign investors act at time t informed by real-time exchange rate movements that aggregate market sentiment.

2.3 Functions and equilibrium requirements

I adapt the Exchange Market Pressure (EMP) framework (Girton and Roper, 1977; Eichengreen et al., 1994) shown in Equation (4) to capture the full spectrum of currency stress. While nominal exchange rates remain artificially stable under a pegged regime, the EMP internalizes the unobservable monetary instruments utilized to defend the parity via reserve depletion or defensive interest rate hikes.

$$EMP_{it} = \frac{\Delta e_{it}}{\sigma_{\Delta e,i}} - \frac{\Delta R_{it}}{\sigma_{\Delta R,i}} + \frac{\Delta r_{it}}{\sigma_{\Delta r,i}} \tag{4}$$

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 incomplete informational game is solved via a sequential Perfect Bayesian Equilibrium (PBE) (Morris and Shin, 1998). Foreign investors dynamically update their prior beliefs regarding the probability of reserve depletion ($R_t < R_{\min}$) and imminent devaluation based on the observed noisy signal ($\mathcal{S}_t$) of the

cyber attack intensity ($D_t \geq \bar{D}$) in Equations (5) and (6):

$$\mu_t = \Pr(R_t < R_{\min} \mid \mathcal{H}_t) \tag{5}$$

$$\mu_t(D_t \geq \bar{D} \mid \mathcal{S}_t) = \frac{\Pr(\mathcal{S} \mid D_t \geq \bar{D}) \cdot \Pr(D_t \geq \bar{D})}{\Pr(\mathcal{S})} \tag{6}$$

2.4 Equilibrium solutions and state transitions

Based on the PBE, the utility functions of the players shape the equilibrium path and yield three core theoretical propositions that map directly to the empirical causal identification strategy:

- **Proposition 1 (Peg Vulnerability and Self-fulfilling Prophecies):** $\beta_{\text{EMP, peg}} > 0$

  When a cyber attack (D_t) occurs under a fixed regime, the central bank's delayed disclosure of true reserve adequacy ($\mathcal{H}_t^{\text{Peg}}$) accelerates Bayesian belief updating toward an impending devaluation ($\mu_t \to 1$) among foreign investors. Anticipating a future parity collapse, investors execute preemptive capital flight ($\kappa_t = \text{Run}$) to maximize expected utility U_{FI}, triggering a self-fulfilling speculative attack. The resulting reserve drain imposes heavy intervention costs (C) on the central bank and significantly increases exchange market pressure (EMP_t). Consequently, the attacker realizes a positive net payoff: $U_{FA}(D_t) = \theta \cdot \mathbb{E}[\text{EMP}_t] - c(D_t) > 0$, which incentivizes recurring cyber attacks against pegged regimes.

- **Proposition 2 (Float Absorption and Transparent Price Discovery):** $\beta_{\text{EMP, float}} = 0$

  Under a floating exchange rate regime, continuous price discovery ($\mathcal{H}_t^{\text{Float}}$) provides instantaneous market feedback on the magnitude of the cyber shock D_t, anchoring investor beliefs ($\mu_t \approx \mu_0$). Nominal exchange rate flexibility absorbs the disruption through continuous, equilibrium-clearing price adjustments. This enables foreign investors to rebalance portfolios smoothly to maximize U_{FI} without triggering speculative runs on the currency ($\kappa_t = \text{Hold}$). Given that the central bank does not deplete reserves to defend an arbitrary parity, intervention losses are avoided and U_{CB} is preserved. Consequently, net exchange market pressure remains statistically indistinguishable from zero. Because $\mathbb{E}[EMP_t] = 0$, the expected payoff of the attacker collapses to $U_{FA} = -c(D_t) < 0$, which eliminates the geoeconomic gain (θ) and deters state-sponsored cyber attacks under a floating regime.

- **Proposition 3 (The Flight-to-Safety Mechanism):** $\beta_{\text{EMP, float}} < 0$

  When Propositions 1 and 2 operate concurrently within global financial networks, floating regimes transition into safe havens during systemic cyber attacks. Transparent price discovery and superior shock absorption induce cross-border capital reallocation away from vulnerable fixed regimes toward flexible currencies, actively dampening exchange market pressure ($\beta_{\text{EMP, float}} < 0$). Furthermore, if the

attacking state maintains a floating regime that absorbs these redirected capital inflows, it extracts an amplified geoeconomic gain $U_{FA}(D_t) \gg 0$.

As players learn and adapt to evolving cyber capabilities, the environment transitions following the Markov state-switching frameworks (Hamilton, 1989; Evans and Honkapohja, 2001) across three structural states ($Z_t \in \{B, F, D\}$):

- **Baseline State ($Z_t = B$):** Standard cyber capabilities where moderate attacks occasionally penetrate baseline defenses, generating normal operational risks.
- **Fragile State ($Z_t = F$):** The attacker escalates to severe cyber attacks, breaching critical financial infrastructure, generating widespread information opacity, and exposing systemic vulnerability. Financial contagion heightens risk aversion toward pegged regimes, turning floating regimes into safe havens.
- **Defensive State ($Z_t = D$):** The central bank hardens cyber security protocols and deploys updated threat intelligence to prevent systemic breaches. Consequently, the attacker's payoff U_{FA} collapses across all exchange rate regimes as the cost function $c(D_t)$ dominates, effectively bounding the attacker's equilibrium strategy to routine cyber operations.

Although true cyber capabilities remain unobservable, the transition across these states is driven by the evolution of endogenous defenses and the rational, forward-looking belief formation of market participants.

3 Data and Summary Statistics

To empirically evaluate the theoretical assertions of the game model, I utilize a panel of 30 emerging market economies observed monthly from 2015 to 2024 ($T = 120$). Focusing on emerging markets provides an ideal laboratory; unlike advanced safe-haven economies, emering markets posses a diverse array of de facto exchange rate regimes and exhibit high structural exposure to sudden capital flight. The sample incorporates a geographically diverse cross-section across the African, Asian, East-European, Latin American, and Middle East and North Africa (MENA) regions. This broad geographic coverage ensures that the empirical estimates capture systemic global macro-financial dynamics rather than localized trajectories. To preserve sample homogeneity, I exclude countries experiencing extreme extra-economic dislocations, such as total institutional financial collapse, war mobilization, reliance on sovereign wealth funds for financial stabilization, or severe structural data gaps.

Crucially, while the outcome variable (EMP_{it}) is measured at the country-month level, the systemic cyber shock metric (D_t) is constructed as a global aggregate of operational cyber incidents, including those executed in active conflict zones. Aggregating cyber operations at the global level allows the capture of surges in state-sponsored cyber initiatives while guaranteeing that domestic financial market pressure (EMP_{it}) is not confounded by local physical war campaigns or severe economic sanctions. Analyzing a systemic global shock independent of domestic macro-financial conditions eliminates confounding origin effects and mitigates selection biases driven by localized strategic targeting. Furthermore, owing to deep financial network interconnectivity and cross-border flows, systemic cyber shocks transmit through the global financial system even when a specific emerging market is not the direct target. Domestic endogeneity and reverse causality are naturally mitigated when the shock is a globally aggregated phenomenon.

The 2015-2024 timeframe captures a critical geoeconomic epoch characterized by an unprecedented escalation in state-sponsored cyber operations, sophisticated infrastructure targeting, and systemic cyber risk exposure. I construct a monthly panel to capture the aggregate macro-financial footprint of high-velocity, episodic nature cyber events. The occurrence of systemic global cyber shocks is determined externally, ensuring exogenous timing and isolating the capture of financial contagion.

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 policy. As specified in Equation (4), $EMP_{it} = \frac{\Delta e_{it}}{\sigma_{\Delta e,i}} - \frac{\Delta R_{it}}{\sigma_{\Delta R,i}} + \frac{\Delta r_{it}}{\sigma_{\Delta r,i}}$. 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.

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.

I quantify operational systemic cyber shocks targeting financial infrastructure using global cyber event frequency data provided by the Center for Governance of Technology and Systems (Harry and Gallagher, 2018). The 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, the Deutsche Bundesbank, the Bank of Japan, and Banco de España. This 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. I strictly isolate operational cyber attacks targeting the financial sector, which include: (a) external denial-of-service attacks (e.g., BGP hijacking, ICMP/SYN floods, and Ping of Death); (b) message and interface manipulation (e.g., social media account hijacking and website defacement); (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 attacks (e.g., PLC manipulation and industrial control system intrusions).

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 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.

Table (1) presents the summary statistics for the 30 emerging market economies observed from 2015 to 2024:

Table 1: Summary Statistics across Exchange Rate Regimes

	Full Sample			Pegged Regimes			Floating Regimes		
Variable	**Obs**	**Mean**	**SD**	**Obs**	**Mean**	**SD**	**Obs**	**Mean**	**SD**
Exchange Market Pressure, Z-Score (EMP)	3,419	0.067	1.921	1,184	0.072	1.931	2,235	0.064	1.916
Nominal Depreciation (% MoM, Δe)	3,600	0.519	4.256	1,305	0.746	5.492	2,295	0.390	3.351
Foreign Reserves Change (% MoM, ΔR)	3,421	0.435	5.092	1,184	0.538	4.433	2,237	0.380	5.409
Policy Rate Change (pp, Δr)	3,598	0.034	1.337	1,305	0.023	1.811	2,293	0.040	0.969
Global Cyber Attack Incidents (D)	3,600	11.917	9.986	1,305	12.011	10.105	2,295	11.863	9.920
Global Cyber security Index ($\overline{GCI}$)	3,600	−0.012	0.860	1,305	−0.357	1.092	2,295	0.184	0.615
Inflation Rate (% per annum)	3,564	0.562	1.284	1,292	0.737	1.829	2,272	0.463	0.810
Real GDP Growth Rate (% YoY)	3,570	3.106	5.556	1,284	2.897	4.467	2,286	3.224	6.080

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. Source: Author calculations.

Table 1 reveals crucial time-series variations and structural disparities suitable for identifying exchange market stress response to cyber operational risks over the sample period. Notably, the primary outcome variable, Exchange Market Pressure (EMP), exhibits a sample mean of 0.067 with a standard deviation of 1.921, while the primary treatment variable, global cyber attack incidents (D), records a mean of 11.917 incidents with a standard deviation of 9.986.

Comparing the panel's summary statistics details the distribution of exchange rate regimes, where floating regimes represent 63.75% of the active panel (N = 2,295) and fixed regimes account for 36.25% (N = 1,305). Both regime categories easily exceed standard asymptotic sample thresholds, ensuring sufficient statistical power for local projections and robust country-clustered standard errors. Furthermore, the volatility of exchange rate pressure remains virtually identical across regimes ($SD = 1.931$ for pegs and $SD = 1.916$ for floats), confirming balanced dependent variable distributions prior to estimation.

Crucially, the average of incidence of global cyber attacks (D) is identical across the fixed (12.011) and floating (11.863) regime sub-samples. this confirms that operational cyber shocks are strictly exogenous to domestic exchange rate policies and that cyber attackers do not systematically target countries based on their exchange rate regimes.

Finally, the mean Global Cyber security index highlights a significant divergence in institutional readiness, as floating regimes exhibit a higher baseline resilience compared to fixed regimes ($\overline{GCI} = 0.184$ for floats versus -0.357 for pegs). This divergence suggests that fixed regimes remain closely associated with legacy financial infrastructure that relies heavily on central bank stabilization mechanisms. In contrast, the absence of a state-backed currency parity under floating regimes forces the private sector to internalize risk and develop robust cyber security infrastructure. Because daily exposure to currency volatility demands sophisticated digital hedging, high-frequency trading, automated clearing, and continuous market monitoring,

making high cyber security readiness a matter of structural survival for the private sector. To ensure this structural divergence does not confound the primary treatment effect, this index is strictly partialled out within the first-stage Double Machine Learning (DML) nuisance equations.

4 Empirical Identification Strategy

To empirically test the three game-theoretic propositions, I employ a state-dependent Double Machine Learning Local Projections (DML-LP) approach. Standard linear panel specifications fail to capture the nonlinear, high-velocity, and asymmetric transmission of systemic cyber shocks to financial markets, often suffering from severe endogeneity and model misspecification bias. To overcome these limitations, I integrate the DML causal inference framework (Chernozhukov et al., 2018) with Local Projections (Jordà, 2005), conditioned on pre-treatment exchange rate regime classifications and threshold indicators. This regime-dependent 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 regime-specific 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, and prevent reverse causality, all macroeconomic covariates and regime indicators are lagged by one period ($t-1$). Rather than incorporating standard high-cardinality country fixed effects, which cause overfitting and mechanically absorb treatment variation in machine learning, I embed the Correlated Random Effects (CRE) transformation (Mundlak, 1978) directly within the machine learning first-stage nuisance equations, following the framework (Chiboub and Sadok, 2026). This CRE framework models unobserved, time-invariant country heterogeneity by including country-specific temporal averages of all time-varying controls, alongside pre-treatment lags to eliminate serial correlation and month fixed effects to absorb baseline global macroeconomic shocks. While the time fixed effects completely partial out average global trends, the state-dependent estimates isolate the cross-sectional amplification across regimes. This strategy strictly controls for unobserved global macroeconomic

confounders while preserving the heterogeneous impacts between states.

Specifically, the first-stage DML nuisance equations are estimated over the high-dimensional feature vector W_{it} defined in Equation (7):

$$W_{it} = \left[\mathbf{Z}_{i,t-1}, \ldots, \mathbf{Z}_{i,t-p}, \overline{\mathbf{Z}}_i, \overline{GCI}_i, \text{Month}_t\right] \tag{7}$$

Where $\mathbf{Z}_{i,t-1}$ is the vector of one-period lagged macroeconomic control variables (interest rate differentials, real GDP growth rates, inflation rates, 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 time means of the control variables (Mundlak correlated random effects terms)
$\overline{GCI}_i$ represent the time-invariant Global Cyber security index
Month_t is the vector of month fixed effects.

To identify asymmetric regime effects while maintaining Neyman orthogonality, I follow the heterogeneous treatment framework of Semenova and Chernozhukov (2021), where the primary shock D_{it} is divided into two exclusive and regime-interacted treatment components: $T_{it}^{\text{float}} = D_{it} \times \text{Float}_{i,t-1}$ and $T_{it}^{\text{peg}} = D_{it} \times \text{Peg}_{i,t-1}$. In the first stage, for each forward horizon $h \in \{0, 1, \ldots, 5\}$, the nuisance equations for the outcome and both treatment components are estimated via 4-fold cross-fitting ($K = 4$) using Random Forest regressors ($n_{\text{tree}} = 100$, max_depth = 4) (Breiman, 2001). This prevents overfitting, eliminates sample-splitting bias, and optimizes predictive power in Equations (8), (9), and (10):

$$Y_{i,t+h} = g_0^h(W_{it}) + U_{i,t+h}^h, \quad \mathbb{E}[U_{i,t+h}^h \mid W_{it}] = 0 \tag{8}$$

$$T_{it}^{\text{float}} = m_{0,\text{float}}(W_{it}) + V_{it}^{\text{float}}, \quad \mathbb{E}[V_{it}^{\text{float}} \mid W_{it}] = 0 \tag{9}$$

$$T_{it}^{\text{peg}} = m_{0,\text{peg}}(W_{it}) + V_{it}^{\text{peg}}, \quad \mathbb{E}[V_{it}^{\text{peg}} \mid W_{it}] = 0 \tag{10}$$

Where $Y_{i,t+h}$ is the outcome variable projected at future horizons $T_{i,t}$ are the regime-interacted treatment components $g_0(\cdot)$ and $m_0(\cdot)$ represent the optimal non-parametric machine learning mapping functions.

Centered and orthogonalized residuals are isolated from out-of-fold predictions to detect unexpected innovations in both the outcome and treatment variables that are strictly uncorrelated with the macroeconomic confounders, as defined in Equations (11), (12), and (13):

$$\tilde{Y}_{i,t+h} = Y_{i,t+h} - \hat{g}_0^{h,-k}(W_{it}) \tag{11}$$

$$\tilde{T}_{it}^{\text{float}} = T_{it}^{\text{float}} - \hat{m}_{0,\text{float}}^{-k}(W_{it}) \tag{12}$$

$$\tilde{T}_{it}^{\text{peg}} = T_{it}^{\text{peg}} - \hat{m}_{0,\text{peg}}^{-k}(W_{it}) \tag{13}$$

4.2 Second-stage regime-dependent DML-LP setup

In the second stage, the regime-dependent impulse responses are identified by regressing the orthogonalized outcome residual on the orthogonalized treatment residuals without an intercept, as specified in Equation (14):

$$\tilde{Y}_{i,t+h} = \beta_{\text{float}}^h \tilde{T}_{it}^{\text{float}} + \beta_{\text{peg}}^h \tilde{T}_{it}^{\text{peg}} + \epsilon_{i,t+h}^h \tag{14}$$

Where $\text{Float}_{i,t-1}$ takes a value of 1 if country i maintains a floating exchange rate regime at time $t-1$; $\text{Peg}_{i,t-1} = 1 - \text{Float}_{i,t-1}$ takes a value of 1 if the country i maintains a fixed exchange rate regime. The omission of a linear constant avoids the dummy variable trap and prevents perfect multicollinearity, as first-stage DML residuals are centered at an expected mean of zero by design.

The dynamic, regime-specific Impulse Response Functions (IRFs) are tracked across horizons by the parameter vectors $\Phi_{\text{float}} = \{\beta_{\text{float}}^0, \ldots, \beta_{\text{float}}^5\}$ and $\Phi_{\text{peg}} = \{\beta_{\text{peg}}^0, \ldots, \beta_{\text{peg}}^5\}$. Standard errors are estimated using robust sandwich covariance estimators clustered at the country level (Huber, 1967; White, 1980), as shown in Equation (15):

$$\text{Var}(\hat{\beta}^h) = (\mathbf{M}^T\mathbf{M})^{-1} \left(\sum_{c \in C} \mathbf{M}_c^T \hat{\epsilon}_c^h (\hat{\epsilon}_c^h)^T \mathbf{M}_c \right) (\mathbf{M}^T\mathbf{M})^{-1} \tag{15}$$

Where $\mathbf{M} = [\tilde{T}^{\text{float}}, \tilde{T}^{\text{peg}}]$ is the second-stage regressor matrix of orthogonalized treatment signals, c indexes country clusters.

As robustness checks, Lasso and Extreme Gradient Boosting (XGBoost) are evaluated under an identical two-stage cross-fitting framework Tibshirani (1996); Chen and Guestrin (2016).

To formally test for structural asymmetry between exchange rate regimes, I employ a Wald test of linear restrictions. As (Gelman and Stern, 2006) emphasize, observing a statistically significant coefficient in one regime and an insignificant coefficient in another is mathematically insufficient to prove that the two responses are fundamentally asymmetric. The validity of employing this standard statistical inference within this framework is guaranteed by the DML estimator, which relies on sample splitting and Neyman

orthogonalization to ensure asymptotic normality Chernozhukov et al. (2018).

4.3 Modeling nonlinear threshold effects

Because high-intensity cyber attacks may breach the shock-absorbing capacity of exchange rate regimes, while low-intensity operations may fall below the threshold of market salience, I extend the baseline regime-specific DML-LP framework into a nonlinear interaction structure. To capture state dependence across the distribution of attacks, I define two structural threshold indicators—a high-intensity attack state (Severe_{it}) and a low-intensity defensive state (Minor_{it}) in Equation (16):

$$\text{Severe}_{it} = \mathbb{I}(D_{it} \geq \tau_{90}); \quad \text{Minor}_{it} = \mathbb{I}(0 < D_{it} \leq \tau_{20}) \tag{16}$$

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_{90} as the 90th percentile of strictly positive cyber event counts across the panel. Conversely, τ_{20} is defined as the 20th percentile, isolating routine operational background noise. Setting these thresholds at the outer tails of the distribution aligns with established macro-finance literature on tail-risk events and financial vulnerability (Eichengreen et al., 2011). Furthermore, to ensure that the empirical identification is not an artifact of specific threshold selection, I evaluate alternative threshold specifications for both minor and severe attacks, with detailed results reported in Appendix A.

Following the Neyman orthogonality framework for heterogeneous treatment effects, I evaluate each nonlinear state $s \in \{\text{severe}, \text{minor}\}$ by partitioning the shock D_{it} into four regime- and state-dependent treatment signals. For a given state indicator $S_{it} \in \{\text{Severe}_{it}, \text{Minor}_{it}\}$, the treatment components are constructed in Equations (17) through (20), following the state-dependent Local Projection framework (Auerbach and Gorodnichenko, 2012; Ramey and Zubairy, 2018):

$$T_{it}^{\text{peg, base}} = D_{it} \times \text{Peg}_{i,t-1} \tag{17}$$

$$T_{it}^{\text{peg},s} = D_{it} \times \text{Peg}_{i,t-1} \times S_{it} \tag{18}$$

$$T_{it}^{\text{float, base}} = D_{it} \times \text{Float}_{i,t-1} \tag{19}$$

$$T_{it}^{\text{float},s} = D_{it} \times \text{Float}_{i,t-1} \times S_{it} \tag{20}$$

In the first stage of the DML procedure, all four treatment components and the lead outcome $Y_{i,t+h}$ are purged of the high-dimensional conditioning space W_{it} independently using Random Forest estimators

(Breiman, 2001) ($n_{\text{tree}} = 100, \text{max_depth} = 4$) across $K = 4$ cross-fitting folds. This yields centered, orthogonalized residuals: $\tilde{T}_{it}^{\text{peg, base}}$, $\tilde{T}_{it}^{\text{peg},s}$, $\tilde{T}_{it}^{\text{float, base}}$, $\tilde{T}_{it}^{\text{float},s}$, and $\tilde{Y}_{i,t+h}$.

In the second stage, for each horizon $h \in \{0, 1, \ldots, 5\}$ and state $s \in \{\text{severe}, \text{minor}\}$, the orthogonalized outcome residual $\tilde{Y}_{i,t+h}$ is regressed on the vector of treatment residuals following Chernozhukov et al. (2018), omitting a constant to avoid collinearity:

$$\tilde{Y}_{i,t+h} = \beta^h_{\text{peg, base}} \tilde{T}_{it}^{\text{peg, base}} + \delta^h_{\text{peg},s} \tilde{T}_{it}^{\text{peg},s} + \beta^h_{\text{float, base}} \tilde{T}_{it}^{\text{float, base}} + \delta^h_{\text{float},s} \tilde{T}_{it}^{\text{float},s} + \epsilon^h_{i,t+h} \tag{21}$$

where $\beta^h_{\text{peg, base}}$ and $\beta^h_{\text{float, base}}$ capture the baseline response of Exchange Market Pressure (EMP) during moderate cyber activity. The parameters $\delta^h_{\text{peg},s}$ and $\delta^h_{\text{float},s}$ capture the incremental regime-dependent response specific to tail state s.

The total dynamic impulse response functions (IRFs) combine the baseline and state-specific parameters to evaluate the full transmission of state s shocks across forward horizons:

$$\text{Total Response}^h_{\text{peg},s} = \hat{\beta}^h_{\text{peg, base}} + \hat{\delta}^h_{\text{peg},s} \tag{22}$$

$$\text{Total Response}^h_{\text{float},s} = \hat{\beta}^h_{\text{float, base}} + \hat{\delta}^h_{\text{float},s} \tag{23}$$

Standard errors for these total linear combinations are computed directly from the second-stage clustered covariance matrix $\hat{\Omega}_{\text{cluster}}$ (Huber, 1967; White, 1980), accounting for the covariance between baseline and regime interaction parameters:

$$\text{SE}\left(\hat{\beta}^h_{\text{regime, base}} + \hat{\delta}^h_{\text{regime},s}\right) = \sqrt{\widehat{\text{Var}}(\hat{\beta}^h_{\text{regime, base}}) + \widehat{\text{Var}}(\hat{\delta}^h_{\text{regime},s}) + 2 \cdot \widehat{\text{Cov}}(\hat{\beta}^h_{\text{regime, base}}, \hat{\delta}^h_{\text{regime},s})} \tag{24}$$

5 Empirical Results

5.1 Baseline estimates: the transmission of cyber attacks

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 (2) 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 2: 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})				
Global Cyber Attack Incidents (D)	-3.7667^{***}	0.0001	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	$I(0)$

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 regime-dependent Double Machine Learning Local Projections (DML-LP) approach to isolate the dynamic and asymmetric responses of exchange market pressure (EMP) to global cyber attacks (D) across different exchange rate regimes. Figure (1) maps the resulting baseline impulse responses. Furthermore, to mitigate machine learning misspecification and ensure the robustness of the baseline estimates, Table (3) presents alternative estimations utilizing Lasso regularized regression (Tibshirani, 1996; Hastie, 2009) and Extreme Gradient Boosting (XGBoost) (Chen and Guestrin, 2016).

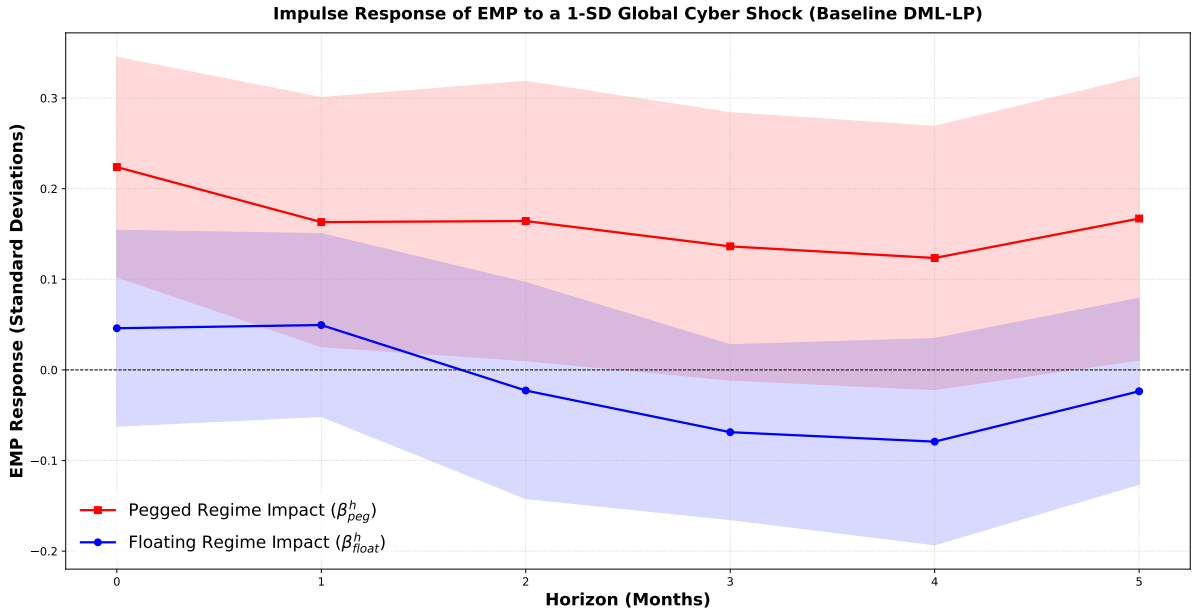


Figure 1: Asymmetric IRF of Exchange Market Pressure to Cyber Attacks across Exchange Rate Regimes

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 global cyber attacks (1 SD corresponds to 10 incidents). Standard errors are clustered at the country level to account for autocorrelation and heteroskedasticity. The estimation utilizes a Hybrid-Mundlak configuration containing country-specific historical time-means, pre-treatment lags, and explicit month fixed effects embedded within the first-stage Double Machine Learning nuisance architecture. Source: Author calculations

Table 3: Baseline State: Asymmetric EMP Response to a 1-SD Global Cyber Attack and Robustness Checks across Learners

	$h=0$	$h=1$	$h=2$	$h=3$	$h=4$	$h=5$
Panel A: Baseline Random Forest						
Pegged Regime (β_{peg})	0.224***	0.163**	0.164**	0.136*	0.124*	0.167**
	(0.062)	(0.070)	(0.079)	(0.075)	(0.074)	(0.080)
Floating Regime (β_{float})	0.046	0.050	-0.023	-0.069	-0.079	-0.024
	(0.055)	(0.051)	(0.061)	(0.049)	(0.058)	(0.052)
Wald Test: $\beta_{\text{float}} = \beta_{\text{peg}}$ (p-value)	[0.030**]	[0.182]	[0.052*]	[0.022**]	[0.026**]	[0.039**]
Panel B: XGBoost Estimator						
Pegged Regime (β_{peg})	0.219***	0.211**	0.116	0.115	0.130	0.144
	(0.074)	(0.089)	(0.089)	(0.085)	(0.099)	(0.101)
Floating Regime (β_{float})	0.020	0.064	-0.103	-0.104	-0.132*	-0.065
	(0.075)	(0.065)	(0.081)	(0.067)	(0.079)	(0.078)
Wald Test: $\beta_{\text{float}} = \beta_{\text{peg}}$ (p-value)	[0.034**]	[0.122]	[0.041**]	[0.026**]	[0.018**]	[0.052*]
Panel C: Lasso Estimator						
Pegged Regime (β_{peg})	0.214	0.274	0.143	0.186	0.154	0.068
	(0.258)	(0.234)	(0.225)	(0.215)	(0.241)	(0.225)
Floating Regime (β_{float})	0.091	0.150	-0.027	0.027	-0.010	-0.084
	(0.271)	(0.226)	(0.249)	(0.221)	(0.259)	(0.243)
Wald Test: $\beta_{\text{float}} = \beta_{\text{peg}}$ (p-value)	[0.069*]	[0.084*]	[0.016**]	[0.041**]	[0.046**]	[0.035**]
Observations	3,164 to 3,303					
Correlated Random Effects	Yes					
Month Fixed Effects	Yes					
Pre-treatment Lags	Yes					

Notes: Local projections estimates. The response is measured in standard deviations to a one-standard-deviation exogenous shock in global cyber attacks (1 SD refer to 10 incidents). Wald test p-values are testing the null hypothesis of cross-regime equality. Standard errors, clustered at the country level, are reported in parentheses. Significance levels: $^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. Random Forest is the baseline DML estimator, while Lasso and XGBoost serve as robustness checks. All models include pre-treatment lags, cross-sectional country means, and continuous time trends. Source: Author calculations.

Results under the baseline state B demonstrate a pronounced asymmetric response across exchange rate regimes, formally confirmed by Wald tests of cross-regime equality. Under a pegged regime, pricing uncertainty regarding potential losses combined with precarious foreign reserve adequacy implies that a 1-SD cyber shock generates a statistically significant positive response in exchange market pressure (EMP). This pressure peaks immediately upon impact ($h = 0 : \beta_{\text{peg}} = 0.224^{***}$). Considering that standard crisis literature defines a speculative currency crisis by an exchange market pressure surge of at least 2 standard deviations (Eichengreen et al., 1994), an isolated cyber attack accounts for over 11% of the entire crisis threshold on impact. This confirms Proposition 1 ($\beta_{\text{EMP, peg}} > 0$), illustrating peg vulnerability and the risk of self-fulfilling speculative attacks.

This immediate pressure surge reflects the institutional vulnerability of defending a fixed parity with

finite foreign reserves and destabilizing interest rates hikes. It aligns with second-generation currency crisis models where forward-looking foreign investors rationally run on the currency before foreign reserves are fully depleted (Obstfeld, 1984, 1996). While pegged regimes frequently employ capital controls to mitigate capital flight under the impossible trinity (Mundell, 1963; Fleming, 1962), such administrative restrictions are easily circumvented during stress episodes through trade misinvoicing and parallel exchange markets (Edwards, 1999). The resulting parallel market premium accelerates capital flight amid acute currency overvaluation and heightened devaluation risk (Dornbusch et al., 1995; Frankel and Rose, 1996), compounding the initial cyber shock.

Conversely, the baseline state B yields statistically insignificant estimates for the floating regime, confirming Proposition 2 ($\beta_{\text{EMP, float}} = 0$) regarding shock-absorption and nominal adjustment capacity. Continuous price discovery in flexible exchange rates transparently reveals the loss market value of the currency, mitigating loss uncertainty and preventing generalized panic. This finding corroborates foundational open-economy literature showing that floating regimes provide immediate shock buffering through instantaneous price adjustments (Edwards and Yeyati, 2005), eliminating the classic 'one-way bet' that speculators exploit under fixed pegs. Although open capital accounts under floating regimes allow for swift portfolio reallocation (Mundell, 1963; Fleming, 1962), this regime flexibility relieves cumulative exchange market pressure by preventing persistent currency overvaluation and divergence from the parallel market rate, which would otherwise induce speculative hoarding.

Although, the Wald test confirms structural asymmetry between these exchange rate regimes, Proposition 3 of a flight-to-safety mechanism is not fully satisfied in these baseline state, as the response of the floating regime remains indistinguishable from zero.

Robustness exercises using the XGBoost estimator confirm that the sign and statistical significance of these responses persist across the immediate horizons ($h = 0$ and $h = 1$). In contrast, the standard linear Lasso is unable to capture these interaction effects. This divergence indicates that traditional linear specifications struggle to detect higher-order dependencies, underscoring the importance of deploying flexible non-parametric machine learning methods (such as gradient boosting and random forests) to accommodate multidimensional and nonlinear transmission channels.

5.2 Nonlinearities: severe vs minor cyber attacks

To stress-test these findings under different states Z, I evaluate the impact of severe cyber attacks on exchange market pressure across regimes using the unified 4-treatment DML-LP framework. Figure (2) plots the regime-dependent impulse responses, while Table (4) reports the corresponding estimates and

robustness checks across alternative learners:

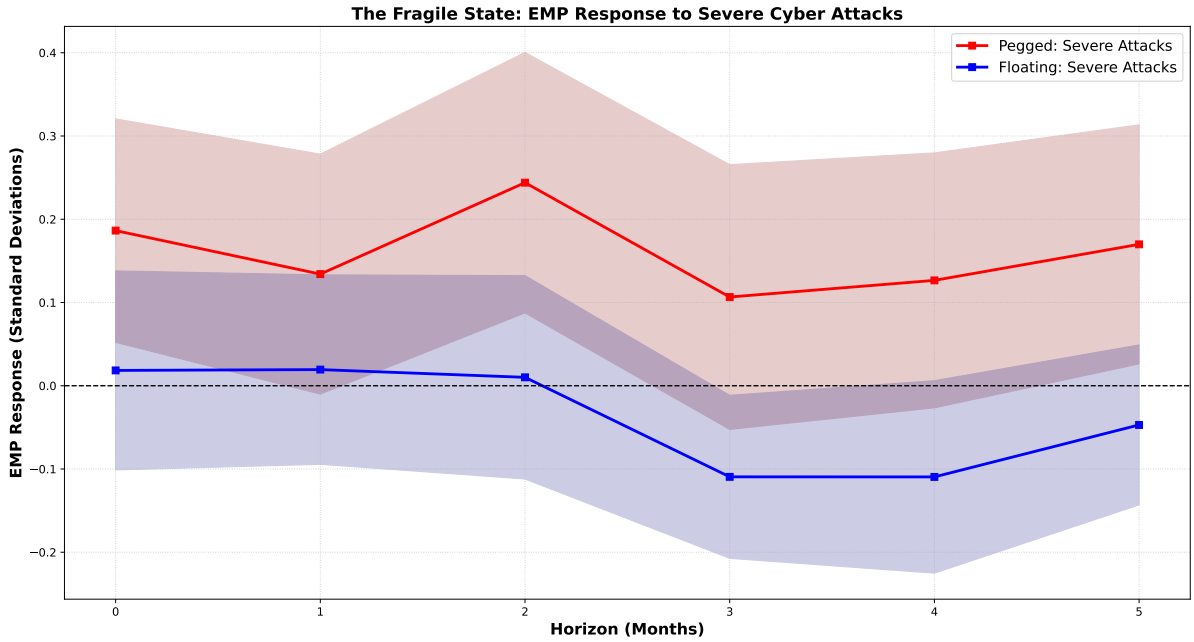


Figure 2: Nonlinear IRF of Exchange Market Pressure to Severe Cyber Attacks across Exchange Rate Regimes

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 global cyber attacks (1 SD corresponds to 10 incidents). Standard errors are clustered at the country level to account for autocorrelation and heteroskedasticity. The estimation utilizes a Hybrid-Mundlak configuration containing country-specific historical time-means, pre-treatment lags, and explicit month fixed effects embedded within the first-stage Double Machine Learning nuisance architecture. Source: Author calculations.

Table 4: The Fragile State: EMP Nonlinear Response to a 1-SD Minor Global Cyber Attack and Robustness Checks across Learners

	Random Forest			**XGBoost**			**Lasso**		
Horizon (h)	**Pegged**	**Floating**	**Wald (p)**	**Pegged**	**Floating**	**Wald (p)**	**Pegged**	**Floating**	**Wald (p)**
$h = 0$	0.186***	0.018	0.065*	0.216	0.015	0.178	0.243	0.123	0.095*
	(0.068)	(0.061)		(0.139)	(0.138)		(0.581)	(0.595)	
$h = 1$	0.134*	0.019	0.196	0.108	-0.043	0.237	0.154	0.032	0.100
	(0.074)	(0.058)		(0.143)	(0.145)		(0.488)	(0.482)	
$h = 2$	0.244***	0.010	0.016**	0.500***	0.216*	0.032**	0.363	0.186	0.013**
	(0.080)	(0.062)		(0.149)	(0.123)		(0.450)	(0.451)	
$h = 3$	0.107	-0.109**	0.022**	0.022	-0.263**	0.034**	0.019	-0.142	0.044**
	(0.081)	(0.050)		(0.148)	(0.107)		(0.440)	(0.432)	
$h = 4$	0.127	-0.110*	0.011**	0.025	-0.342***	0.004***	0.033	-0.138	0.038**
	(0.078)	(0.059)		(0.136)	(0.117)		(0.462)	(0.467)	
$h = 5$	0.170**	-0.047	0.010**	0.156	-0.127	0.007***	0.196	0.036	0.023**
	(0.073)	(0.049)		(0.104)	(0.099)		(0.349)	(0.361)	
Correlated Random Effects			Yes						
Month Fixed Effects			Yes						
Pre-treatment Lags			Yes						

Notes: Local projections estimates using DML for the cumulative impulse response of EMP to severe global cyber attacks (incidents exceeding the 90th percentile). Standard errors, clustered at the country level, are in parentheses. Significance levels: $^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. Random Forest serves as the baseline DML estimator, while Lasso and XGBoost are provided as robustness checks. All models include pre-treatment lags, cross-sectional country means, and continuous time trends. Source: Author calculations.

Results indicate that under the fragile state S, a 1-SD increase in severe global cyber attacks targeting systemic financial infrastructures generates a statistically significant positive response in EMP under fixed regimes. This pressure peaks at horizon $h = 2$ ($\beta_{\text{peg}}^{\text{severe}} = 0.244^{***}$). This finding strongly reinforces the peg vulnerability outlined in Proposition 1 ($\beta_{\text{EMP, peg}} > 0$). Furthermore, it confirms that the self-fulfilling speculative dynamics modeled by Obstfeld (1984, 1996) is maintained when severe cyber shocks intersect with informational opacity.

In contrast, the shock-absorption mechanism described in Proposition 2 ($\beta_{\text{EMP, float}} = 0$) holds strictly during the immediate impact phase, demonstrating that severe cyber attacks are smoothly absorbed by instant price adjustments. Although the literature shows that floating regimes are highly susceptible to exchange rate volatility (Kočenda and Valachy, 2006) that can quickly escalate into market panic driven by a 'fear of floating' (Calvo and Reinhart, 2002) and openness of capital accounts (Stiglitz, 2000), these empirical results demonstrate a different mechanism. Specifically, the real-time price discovery of a floating regime mitigates uncertainty and instantaneously dissipates market stress, even during severe cyber attacks.

Proposition 3 regarding the fight-to-safety mechanism ($\beta_{\text{EMP, float}} < 0$) is formally confirmed. At the three-month horizon, exchange market pressure responds significantly and negatively to severe global cyber attacks ($h = 3 : \beta_{float} = -0.109^{**}$), corresponding with the continued satisfaction of Propositions 1 and 2 along a statistically significant Wald test across regimes. This indicates that foreign investors dynamically reallocate capital away from pegged regimes burdened with loss uncertainty and toward the relative safety

of transparent floating regimes. However, this relief in exchange market pressure remains brief and does not persist over longer horizons.

Formal Wald tests confirm these structural asymmetries across regimes. While the linear Lasso does not account for higher-order interactions, employing XGBoost captures these complex nonlinear patterns and reveals more pronounced, persistent flight-to-safety dynamics.

A potential concern is that the negative exchange market pressure (EMP) response under floating regimes is confounded by endogenous monetary policy easing, creating the illusion of a flight-to-safety rather than capturing genuine capital inflows and nominal appreciation. To address this, I disaggregate the index and re-estimate the state-dependent DML-LP model exclusively on the interest rate differential (Δr) and the nominal exchange rate depreciation (Δe) components for floating regimes. The results are presented in Table (5):

Table 5: Robustness Check: Separate Component Responses to Severe Cyber Attacks under Floating Regimes

Horizon (h)	**Exchange Rate Depreciation (Δe)**	**Interest Rate Differential (Δr)**
$h = 0$	-0.0047^{**}	0.0033
	(0.0123)	(0.0015)
$h = 1$	0.0036	0.0025
	(0.0137)	(0.0010)
$h = 2$	-0.0060	0.0019
	(0.0063)	(0.0012)
$h = 3$	-0.0230^{***}	0.0010
	(0.0055)	(0.0011)
$h = 4$	-0.0100	0.0007
	(0.0072)	(0.0015)
$h = 5$	-0.0200^{***}	0.0003
	(0.0117)	(0.0015)
Average Observations	3,249	3,247

Notes: Local projections estimates using DML for the isolated impact of severe global cyber shocks (90th percentile) on individual components of the exchange market pressure index under floating regimes. A negative coefficient for Δe indicate exchange rate appreciation. Standard errors clustered at the country level (in parentheses). Significance levels: $^{***}p < 0.01$, $^{**}p < 0.05$. All models contain pre-treatment lags, cross-sectional country means, and continuous time trends. Source: Author calculations

Under severe cyber attacks, the component-level results firmly validate Proposition 3. Crucially, the interest rate responses at the flight-to-safety across all horizons are economically negligible and statistically indistinguishable from zero. Conversely, the exchange rate component exhibits a highly significant negative response ($\beta_{\text{float}}^{\text{severe}} = -0.023, p < 0.01$), indicating sharp nominal appreciation. This verifies that domestic monetary policy cuts are not driving the observed relief in the aggregate exchange market pressure. Rather,

this relief reflects genuine exogenous capital inflows, as the floating regime attracts foreign investors seeking transparent price discovery.

While the traditional asset pricing literature posits that distressed investors overwhelmingly seek lower volatility assets (Sarwar, 2017; Adrian et al., 2019), Proposition 3 reveals a structural nuance. Although pegged regimes artificially insulate nominal exchange rate fluctuations, forward-looking investors seek refuge in the informational transparency of floating regimes, despite being susceptible to larger baseline nominal fluctuations (Kočenda and Valachy, 2006). The well-documented financial domino effect, where stress systematically spills over from one pegged currency to other pegged regimes (Eichengreen et al., 1996; Balke et al., 2024), further incentivizes this herding behavior toward the shock-absorbing float.

Furthermore, to assess sensitivity to threshold selection, I evaluate alternative cutoff parameters up to the 95th percentile, with detailed results reported in Appendix A. The baseline findings remain highly robust to these variations, preserving the core dynamics of peg vulnerability, float shock absorption, and flight-to-safety mechanisms that support Propositions 1 to 3.

Figure (3) plots the regime-dependent impulse responses to minor cyber attacks, while Table (6) reports the corresponding estimates and robustness checks across alternative learners:

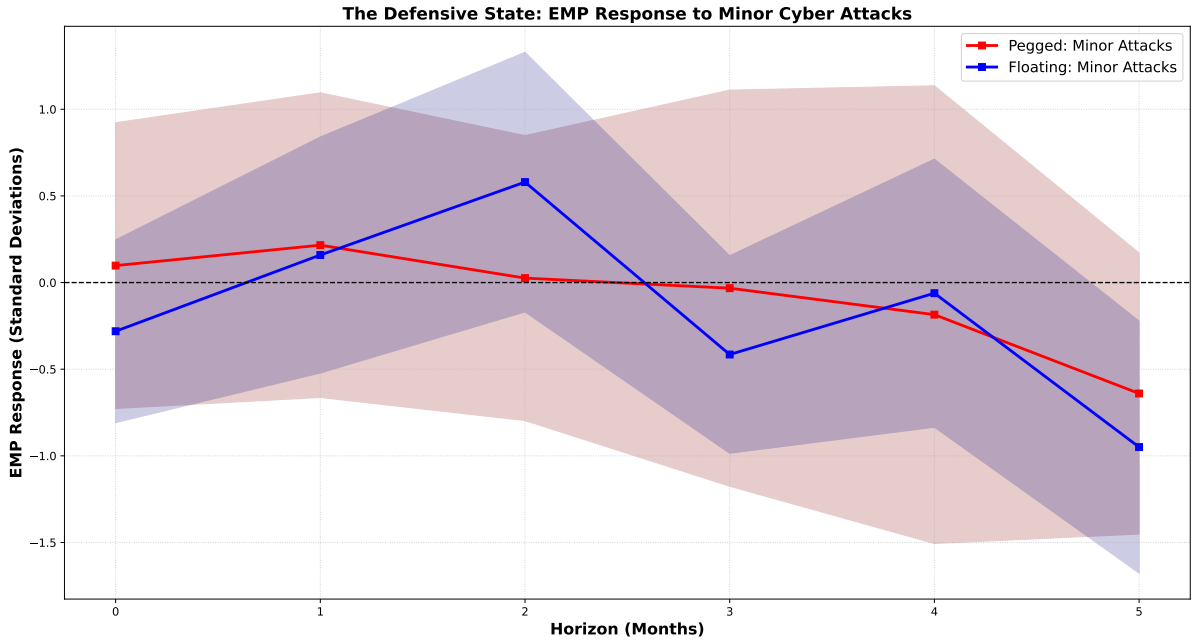


Figure 3: Nonlinear IRF of Exchange Market Pressure to Minor Cyber Attacks across Exchange Rate Regimes

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 global cyber attacks (1 SD corresponds to 10 incidents). Standard errors are clustered at the country level to account for autocorrelation and heteroskedasticity. The DML-LP estimation utilizes a Hybrid-Mundlak configuration containing country-specific historical time-means, pre-treatment lags, and explicit month fixed effects embedded within the first-stage Double Machine Learning nuisance architecture. Source: Author calculations

Table 6: The Defensive State: EMP Nonlinear Response to a 1-SD Minor Global Cyber Attack and Robustness Checks across Learners

	Random Forest			**XGBoost**			**Lasso**		
Horizon (h)	**Pegged**	**Floating**	**Wald** (p)	**Pegged**	**Floating**	**Wald** (p)	**Pegged**	**Floating**	**Wald** (p)
$h = 0$	0.098	-0.281	0.414	0.121	-0.419	0.414	-1.063	-1.430	0.404
	(0.421)	(0.269)		(0.638)	(0.518)		(3.334)	(3.241)	
$h = 1$	0.216	0.159	0.916	0.227	-0.175	0.553	-0.253	-0.660	0.405
	(0.448)	(0.347)		(0.664)	(0.564)		(3.744)	(3.621)	
$h = 2$	0.026	0.580	0.307	-0.379	0.424	0.232	1.868	2.173	0.484
	(0.419)	(0.382)		(0.560)	(0.604)		(3.995)	(4.158)	
$h = 3$	-0.032	-0.415	0.550	-0.090	-0.714	0.439	0.114	-0.229	0.503
	(0.583)	(0.291)		(0.816)	(0.496)		(3.977)	(3.780)	
$h = 4$	-0.185	-0.061	0.869	-0.088	0.143	0.812	-0.112	-0.017	0.887
	(0.674)	(0.395)		(0.959)	(0.677)		(4.664)	(4.524)	
$h = 5$	-0.640	-0.949**	0.601	-0.699	-1.249*	0.513	-0.694	-1.101	0.394
	(0.414)	(0.371)		(0.734)	(0.645)		(4.268)	(4.228)	
Correlated Random Effects			Yes						
Month Fixed Effects			Yes						
Pre-treatment Lags			Yes						

Notes: Local projections estimates using DML for cumulative impulse response of EMP to minor global cyber attacks (incidents under the 20th percentile of positive attack months). Standard errors clustered at the country level (in parentheses). Significance levels: $^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. Random Forest is the baseline DML estimator, while Lasso and XGBoost serve as robustness checks. All models contain pre-treatment lags, cross-sectional country means, and continuous time trends. Source: Author calculations

Results under the Defensive State demonstrate that minor cyber incidents constitute operational background noise rather than systemic threats. The initial and intermediate impulse responses for both floating and fixed regimes are statistically indistinguishable from zero, failing to trigger the financial frictions outlined in Propositions 1 through 3. While the floating regime exhibits a significant negative coefficient at the fifth month ($h = 5$), this isolated and delayed estimation is theoretically implausible, reflecting statistical noise at extended horizons rather than a structural market response to cyber operations. Because the continuous and immediate capital reallocation pattern observed during severe shocks is completely absent, I conclude that under sub-threshold cyber threats, the core structural vulnerabilities of pegged regimes and the flight-to-safety mechanism remain dormant.

Furthermore, shifting the minor incident threshold to the 15th percentile as a sensitivity check yields results consistent with the baseline findings, confirming that routine cyber operations fail to generate exchange market pressure across both exchange rate regimes (reported in Appendix A).

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 (4). By randomizing the chronological timeline of the global 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.

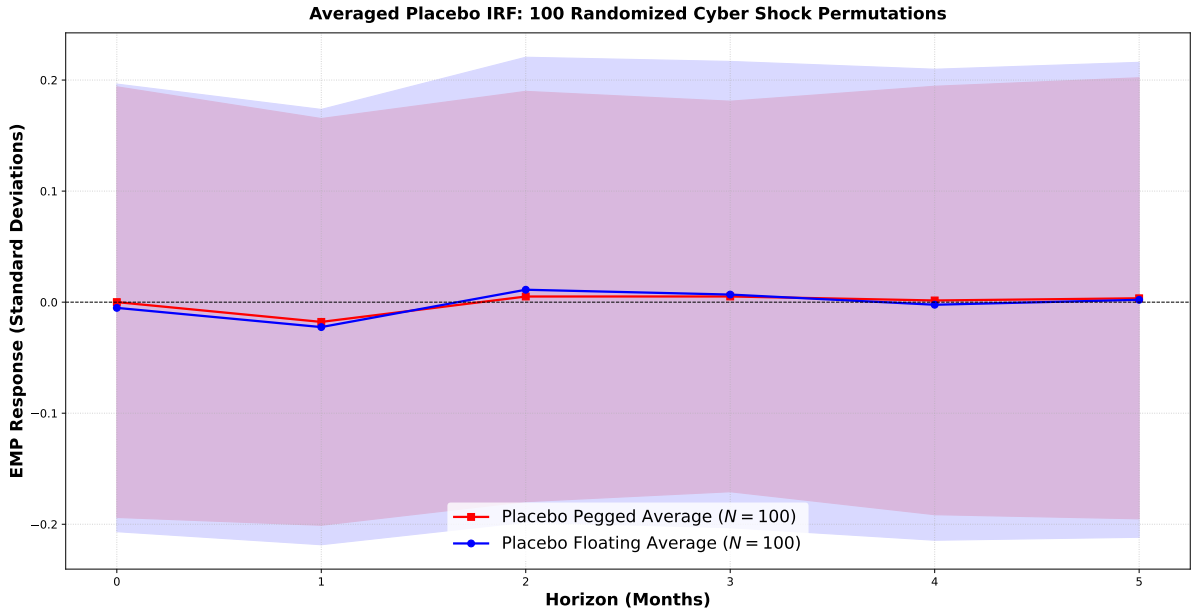


Figure 4: Averaged Placebo IRF: 100 Randomized Cyber Attack Permutations

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 global cyber attacks (1 SD corresponds to 10 incidents). Standard errors are clustered at the country level to account for autocorrelation and heteroskedasticity. The estimation utilizes a Hybrid-Mundlak configuration containing country-specific historical time-means, pre-treatment lags, and explicit month fixed effects embedded within the first-stage Double Machine Learning nuisance architecture. Source: Author calculations

Across all horizons and under both regimes, 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 highly interconnected digital financial infrastructure, the sophistication of systemic cyber operations introduces a critical transmission channel for currency attacks and geoeconomic fragmentation. By inducing systemic financial stress, these shocks exploit information asymmetries and structurally alter the strategic interaction between central banks and foreign investors in the foreign exchange market. While fixed regimes defend an anchor to attract foreign capital, the empirical results demonstrate that this nominal insulation masks actual operational losses and peg sustainability. Traditional monetary trilemma constraints,

such as capital controls and reserve-backed peg defenses, face challenges to bind the rapid reallocation of foreign capital, incentivizing investors to preemptively liquidate their positions. Consequently, the choice of exchange rate regime fundamentally dictates the pricing of cyber risk: pegged regime trade nominal stability for informational uncertainty, whereas flexible regimes exchange higher baseline fluctuations for continuous price discovery that shape capital flows among foreign investors.

While this framework aggregates global cyber attacks against the broad financial system, future research could disaggregate these dynamics by mapping specific micro-structural vulnerabilities in the financial network. Embedding targeted disruptions to wholesale payment systems, centralized clearing houses, or critical third-party cloud infrastructure into sovereign debt and asset pricing models represents a natural progression for the 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

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.

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

Balke, F., A. Barth, A. Reichel, and M. Wahrenburg (2024). Peg abandonment and cross-currency contagion. *Management Science 70*(8), 5599–5606.

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

Boungou, W. (2023). Cyber-attacks and banking intermediation. *Economics Letters 233*, 111354.

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

Calvo, G. A. and C. M. Reinhart (2002). Fear of floating. *The Quarterly journal of economics 117*(2), 379–408.

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

Chen, T. and C. Guestrin (2016). Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, pp. 785–794.

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*.

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.

Dornbusch, R., I. Goldfajn, R. O. Valdés, S. Edwards, and M. Bruno (1995). Currency crises and collapses. *Brookings papers on economic activity 1995*(2), 219–293.

Edwards, S. (1999). How effective are capital controls? *Journal of Economic Perspectives 13*(4), 65–84.

Edwards, S. and E. L. Yeyati (2005). Flexible exchange rates as shock absorbers. *European economic review 49*(8), 2079–2105.

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.

Eichengreen, B., A. K. Rose, and C. Wyplosz (1996). Contagious currency crises.

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.

Evans, G. W. and S. Honkapohja (2001). *Learning and expectations in macroeconomics*. Princeton University Press.

Fleming, J. M. (1962). Domestic financial policies under fixed and under floating exchange rates (politiques finacierieures interieures avec un systeme de taux de change fixe et avec un systeme de taux de change fluctuant)(politica financiera interna bajo sistemas de tipos de cambio fijos o de tipos de cambio fluctuantes). *Staff Papers-International Monetary Fund 9*(3), 369–380.

Frankel, J. A. and A. K. Rose (1996). Currency crashes in emerging markets: An empirical treatment. *Journal of international Economics 41*(3-4), 351–366.

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.

Gelman, A. and H. Stern (2006). The difference between "significant" and "not significant" is not itself statistically significant. *The American Statistician 60*(4), 328–331.

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.

Hamilton, J. D. (1989). A new approach to the economic analysis of nonstationary time series and the business cycle. *Econometrica: Journal of the econometric society*, 357–384.

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

Hastie, T. (2009). The elements of statistical learning: data mining, inference, and prediction.

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.

Kočenda, E. and J. Valachy (2006). Exchange rate volatility and regime change: A visegrad comparison. *Journal of Comparative Economics 34*(4), 727–753.

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

Kotidis, A. and S. L. Schreft (2025). The propagation of cyberattacks through the financial system: Evidence from an actual event. *The Journal of Finance 80*(6), 3313–3358.

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

Mundell, R. A. (1963). Capital mobility and stabilization policy under fixed and flexible exchange rates. *Canadian Journal of Economics and Political Science/Revue canadienne de economiques et science politique 29*(4), 475–485.

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.

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

Semenova, V. and V. Chernozhukov (2021). Debiased machine learning of conditional average treatment effects and other causal functions. *The Econometrics Journal 24*(2), 264–289.

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

Stiglitz, J. E. (2000). Capital market liberalization, economic growth, and instability. *World development 28*(6), 1075–1086.

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.

Tibshirani, R. (1996). Regression shrinkage and selection via the lasso. *Journal of the Royal Statistical Society Series B: Statistical Methodology 58*(1), 267–288.

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.

Zoricakova, J., N. Filickova, and K. Kocisova (2026). Contagion and systemic risk in the european banking sector: implications for sustainable regulation and financial system resilience. *Eurasian Economic Review*, 1–53.

A Online Appendix: Sensitivity Analysis

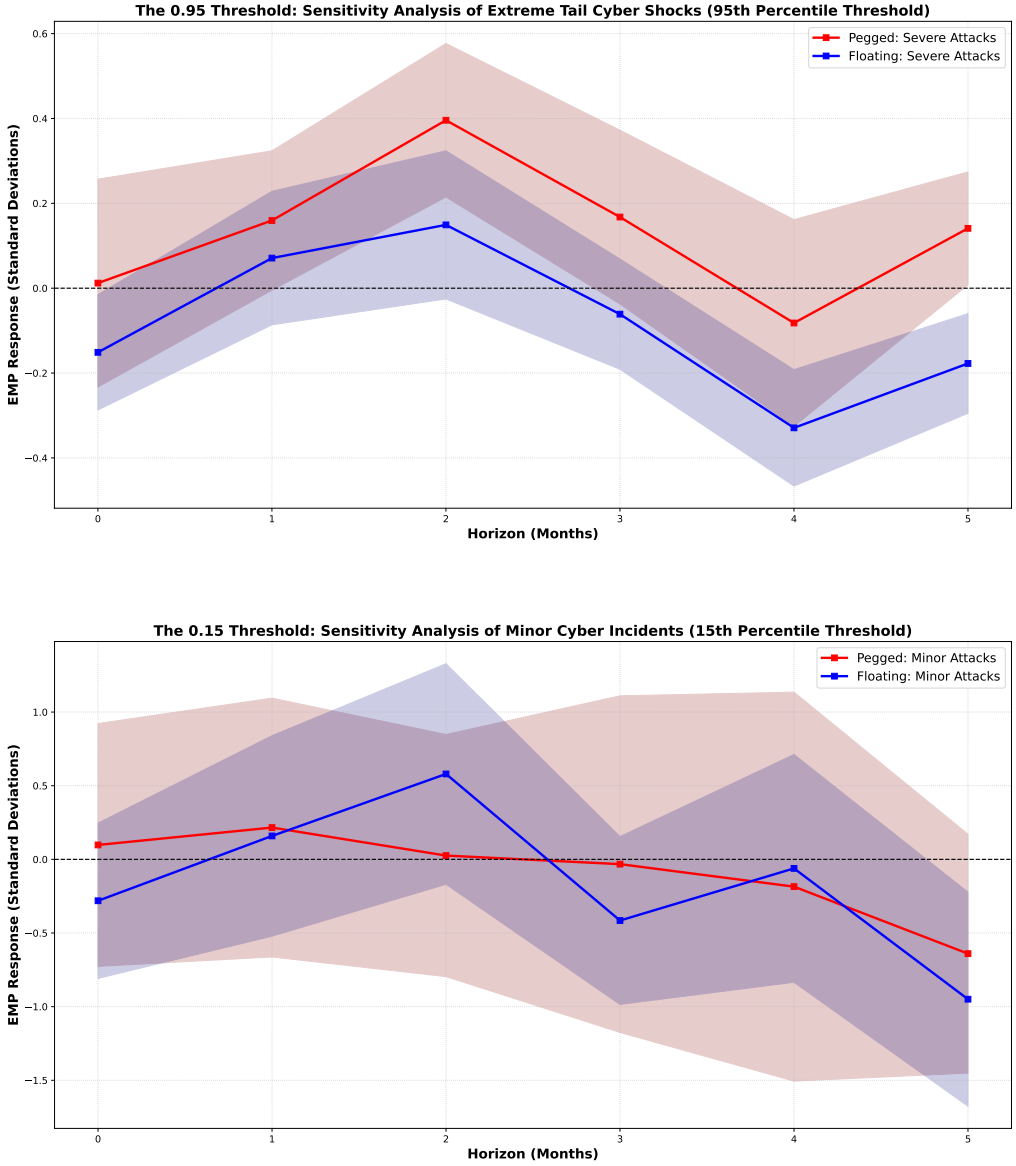


Figure OA.1: Sensitivity Analysis of Cyber Incident Thresholds

Note: Local Projection impulse responses of the Exchange Market Pressure (EMP) index under alternative severity thresholds. The top panel displays the treatment effect utilizing an extreme 95th percentile threshold for systemic attacks, confirming the robustness of the baseline mechanisms. The bottom panel displays the treatment effect utilizing a 15th percentile threshold for minor incidents, confirming the absence of macroeconomic transmission for routine operational disruptions. Source: Author Calculations