Discussion of Short-Circuiting Short-Term Funding

Based on Kahn, Karunamuni & Paddrik

Jorge Miguel Bravo [1]

[1]Professor of Finance and Economics, NOVA IMS Universidade Nova de Lisboa, Lisbon, Portugal & MagIC & Université Paris-Dauphine PSL & LEDa & MagIC & ISCTE-IUL BRU & CEFAGE-UE.

November 18, 2025

Outline

Why Should Macro and Policy Economists Care?

- The U.S. repo market (Tri-party segment) is central to:
  - Short-term dollar funding,
  - Transmission of monetary policy (ON RRP, reserves, policy corridor),
  - Liquidity distribution across dealers and banks.
- The 2019 repo episode showed:
  - Aggregate reserves are not sufficient statistics.
  - **Location and timing** of liquidity, plus market structure, matter for rates.
- Cyber and operational outages can generate *repo-like runs and rate spikes* even with unchanged fundamentals.
- Research question: **If cyberattacks disable important cash lenders in the U.S. tri-party repo market, how big could the resulting funding gaps and rate spikes be, and which institutions matter most?**

Tri-Party Repo in the Monetary Policy Framework

- Non-centrally cleared tri-party repo at BNY Mellon:
  - Lenders: mainly asset managers / MMFs, plus banks and securities lenders.
  - Borrowers: primary dealers, banks, Federal Reserve (via ON RRP).
- Links to policy:
  - ON RRP facility and reserves management.
  - Arbitrage between repo, bills and fed funds.
  - Collateral transformation and distribution of safe assets.
- A cyber shock here is effectively:
  - A sudden, institution-specific constraint on the supply of money-market funding.
  - Potentially a wedge between policy rates and secured funding rates.

Data Overview

- **Repo data:** Transaction-level tri-party repo at holding-company level (2016–2024).
- Key fields:
  - Lender and borrower IDs.
  - Principal amount, collateral type and value.
  - Repo rate, maturity.
  - Intraday settlement time.
- **Cyber data:** BitSight cybersecurity ratings.
  - Overall score (250–900, effective range around 300–820).
  - 16 risk-vector grades (A–F) such as Patching Cadence, Open Ports, SSL, etc.

Stylised Facts

- Repo collateral:
  - U.S. Treasuries $\approx 70\%$ of collateral.
  - Agency MBS and agency debt $\approx 20\%$.
- Participation:
  - ~ 139 lenders, ~ 73 borrowers over sample.
  - Asset managers dominate lending volumes.
- Relationship stability:
  - ~ 680 daily lender–borrower pairs; $\approx 97.5\%$ repeat next day.
  - Cosine similarity measure suggests $< 2\%$ typical change in pairwise volumes.

Overview of the Framework

- Step 1: **Mechanical stress test** of lender outages.
- Step 2: Estimate a **causal mapping** from lost funding to repo rates (Bartik 2SLS).
- Step 3: Convert cyber scores to **outage probabilities**.
- Step 4: **Monte Carlo** distribution of volume and rate outcomes.
- Step 5: Integrate intraday timing and **resilience / recovery** dynamics.
- Aim: a building block for *macro-prudential cyber stress testing* in core funding markets.

Step 1: Baseline Outage Stress Test

- Construct a simple stress test assuming **all lenders equally likely** to suffer a cyber outage.
- For each lender i:
  - Simulate a full-day outage on day t.
  - Set all trades for lender i to zero.
  - Measure disrupted volumes and number of affected borrowers.
- Results give a distribution of impacts across lenders under uniform risk.

Step 2: Volume-to-Rate Mapping (Bartik 2SLS)

- Goal: translate lost funding volume into changes in repo rates.
- Use MMF lending shocks as an instrument for borrower-level funding changes.
- Two-stage approach:
  1. First stage: change in borrower j's repo volume on day t as a function of weighted changes in MMF supply.
  2. Second stage: borrower's repo rate regressed on instrumented volume change.
- Main estimate: losing \$1bn of MMF funding raises rates by several basis points.

Step 3: Cyber-Conditioned Outage Probabilities

- Convert BitSight ratings into **daily outage probabilities**:
  - Choose a baseline probability (e.g. 0.1% per day).
  - Scale up/down by rating bucket using empirical incident ratios.
- For lender i on day t, obtain probability $\theta_{i,t}$.
- Compute **expected** disrupted volume or rate impact:

$$E[\nu_t] = \sum_i \theta_{i,t} \nu_{i,t}.$$

Step 4: Monte Carlo Simulations

- For each trading day:
  - Draw independent outage indicator for each lender using $\theta_{i,t}$.
  - Aggregate disrupted volume and affected borrowers.
  - Use volume-to-rate mapping to compute rate impact.
- Repeat many times (e.g. 10,000 simulations) to obtain:
  - Distribution of disrupted volumes.
  - Distribution of affected borrowers.
  - Distribution of rate spikes.

Step 5: Modelling Resilience and Timing

- Model **recovery time** from outage as exponential with rate λ:

$$P(\text{recovered by } h) = 1 - e^{-\lambda h}.$$

- Vary:
  - Attack start time (e.g. 6 a.m. to 2 p.m.).
  - Average recovery time (1–4 hours).
- Combine with intraday settlement profile to estimate:
  - Peak disruption during the day.
  - Remaining disruption at the 3:30 p.m. unwind.

Outage Impacts Under Uniform Risk

- Single-lender full-day outage:
  - Median volume impact modest; right tail up to \$30–100bn.
  - Median of about 5 borrowers affected; right tail over 20.
- Mapping volume to rates:
  - Large outages can raise market-wide repo rates by tens of basis points.
  - Rate impact distribution also heavily right-skewed.

Who is Systemically Important?

- Combining volumes and cyber risk:
  - **Asset managers** (MMFs) dominate expected disrupted collateral.
  - Bank-dealers and securities lenders matter, but at smaller scale.
- Treasury-backed repos particularly exposed, given their share in collateral.
- Improving cybersecurity of high-volume asset managers yields the largest reduction in expected disruption.

Distribution of Cyber Outcomes

- Expected disrupted volume per day (under baseline probability) is in the low single-digit billions.
- However, simulated tail scenarios:
  - 99th percentile volumes: tens to hundreds of billions.
  - Rate increases: 25–90 basis points.
  - 25–30 borrowers simultaneously affected.
- Heavy right tail: small increase in outage correlation could significantly worsen extremes.

Timing and Recovery Matter

- Most tri-party settlement occurs early in the day.
- Outages starting 6–9 a.m. with slow recovery (3–4 hours) cause the largest peak disruption.
- Even moderate delays may leave substantial unsettled volume by the unwind, especially for afternoon shocks.
- Cyber resilience (recovery speed and backup processes) is as important as baseline cyber hygiene.

Strengths of the Paper

- Integrates cyber risk into a core funding market using real micro data.
- Rich description of tri-party repo structure and intraday timing.
- Transparent, modular stress-testing framework useful for regulators and practitioners.
- Highlights the central role of non-bank institutions (asset managers) in systemic liquidity provision.

Key Limitations and Assumptions

- Outage probabilities:
  - Based on a chosen baseline plus relative risk factors from BitSight.
  - Numerical results sensitive to this calibration.
- Outages assumed independent across institutions and days.
- Focus on tri-party repo only; does not model spillovers to other markets.
- Behavioural responses (network rewiring, precautionary diversification) largely absent.

Econometric and Modelling Questions

- Is the Bartik instrument truly exogenous to borrower-specific conditions?
- How robust is the linear volume-to-rate mapping in extreme stress?
- How would results change with:
  - Correlated outages via common vendors?
  - Activation of central bank standing facilities?
  - Endogenous changes in haircuts and collateral eligibility?

Policy Takeaways

- Cyber and operational risk are **systemic**: they can trigger funding stress similar to credit or collateral shocks.
- Supervisory focus should include:
  - Cyber posture of key liquidity providers (especially asset managers).
  - Operational resilience and recovery times.
  - Critical settlement windows and concentration in infrastructure.
- Framework offers a way to prioritise where marginal improvements in cyber resilience yield the largest systemic benefit.

Discussion Questions for the Workshop

- How realistic is the assumed mapping from cyber scores to outage probabilities?
- Should regulators stress-test **correlated** cyber outages (e.g., major cloud provider failure)?
- How should central banks design and communicate liquidity backstops in a cyber incident?
- Are asset managers' cyber and operational risks adequately covered in current regulation?
- What are the main challenges in extending this framework to other markets or jurisdictions?

Thank you for your attention!

Comments and discussion

Name: Jorge Miguel Bravo
Institution: NOVA IMS – Universidade Nova de Lisboa
Email: jbravo@novaims.unl.pt
Website: https://www.novaims.unl.pt/en/nova-ims/teaching-staff/d/116